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

MELISSA KELLEY on behalf of herself and all others similarly situated,	**COMPLAINT-CLASS ACTION**
Plaintiff,	
v.	
EQUIFAX INC., and EQUIFAX INFORMATION SERVICES, LLC	**No. _____**
	JURY TRIAL DEMANDED
Defendants.	

CLASS ACTION COMPLAINT

Plaintiff Melissa Kelley ("Plaintiff" or "Class Representative"), on behalf of herself and the Classes defined below, alleges the following against Equifax Inc., and Equifax Information Services, LLC ("EISL") (collectively, the "Defendants," "Equifax," or the "Company"), based on personal knowledge as to Plaintiff's conduct and on information and belief as to the acts of others.

I. INTRODUCTION

1. Defendants Equifax Inc. and EISL operate "Equifax," one of the three largest consumer credit reporting agencies in the United States. Plaintiff has been a consumer of Equifax's services and entrusted Defendants with her personal information. Plaintiff brings this action on a class basis alleging violations of the federal Fair Credit Reporting Act, and the Colorado Consumer Protection Act, as well as negligence, negligence per se, and other common law claims. Plaintiff seeks declaratory relief and redress for affected Equifax consumers.

2. Because Plaintiff and the Class entrusted Defendants with their sensitive personal information, Equifax owed them a duty of care to take adequate measures to protect the information entrusted to it, to detect and stop data breaches, and to inform Plaintiff, the Class, and the Colorado Subclass (defined in paragraphs 35-39, below) of data breaches that could expose Plaintiff and the Class to harm. Equifax failed to do so.

3. Equifax acknowledges that, between May 2017 and July 2017, it was the subject of a data breach in which unauthorized individuals accessed Equifax's database and the names, Social Security Numbers, addresses, and other Personally Identifiable Information ("PII") stored therein (hereinafter the "Data Breach"). According to Equifax, the Data Breach affected as many as 145 million people.

Equifax admits that it discovered the unauthorized access on July 29, 2017, but failed to alert Plaintiff and the Class to the fact of the breach until September 7, 2017.

4. The Data Breach was the inevitable result of Equifax's inadequate approach to data security and the protection of the PII that it collected during the course of its business. Defendants knew and should have known of the inadequacy of their own data security. Equifax has experienced similar such breaches of PII on smaller scales in the past, including in 2013, 2016, and even as recently as January 2017. Over the years, Equifax has jeopardized the PII and, as a result, financial information of hundreds of thousands of Americans.

5. Despite this long history of breaches, Defendants have failed to prevent the Data Breach that has exposed the personal information of over 100 million Americans. The damage done to these individuals may follow them for the rest of their lives, as they will have to monitor closely their financial accounts to detect any fraudulent activity and incur out-of-pocket expenses for years to protect themselves from, and to combat, identity theft now and in the future.

6. Equifax knew and should have known the risks associated with inadequate security, and with delayed reporting of the breach. The potential for harm caused by insufficient safeguarding of PII is profound. With data such as that leaked in the Data Breach, identity thieves can cause irreparable and long-lasting damage

to individuals, from filing for loans and opening fraudulent bank accounts to selling valuable PII to the highest bidder.

7. In the case of Defendants' Data Breach, the potential repercussions for consumers are particularly egregious. Privacy researchers and fraud analysts have called this attack "as bad as it gets." "On a scale of 1 to 10 in terms of risk to consumers," it is a 10.[1]

8. Equifax was, or reasonably should have been, aware of the specific vulnerability in its systems as early as March 2017. In or about March 2017, Equifax discovered a vulnerability in its U.S. website: Apache Struts CVE-2017-5638. Despite knowing that this system flaw jeopardized the PII of millions of consumers, Equifax failed to implement an effective patch for at least 9 weeks, and failed to check this known vulnerability regularly to ensure that consumers' information was secure throughout the period of the Data Breach.

9. Defendants failed to inform millions of consumers of the Data Breach until September 7, 2017, over a month after Defendants first discovered it on July 29. While Defendants took no steps at that time to inform the public in the interim, Defendants did not hesitate to protect themselves; at least three Equifax senior

[1] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

executives, including CFO John Gamble, upon information and belief, sold shares worth $1.8 million in the days following the Data Breach.[2]

10. To provide relief to the millions of people whose PII has been compromised by the Data Breach, Plaintiff Melissa Kelley brings this action on behalf of herself and all others similarly situated. Plaintiff seeks to recover actual and statutory damages, equitable relief, restitution, reimbursement of out-of-pocket losses, other compensatory damages, credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to improve its data security and bring to an end its long history of breaches at the cost of consumers.

II. THE PARTIES

A. PLAINTIFF

11. Plaintiff Melissa Kelley is an individual consumer who has resided in Aurora, Colorado since 2016. Plaintiff engaged, or authorized the engagement of, Equifax on various occasions over the years. As a result, Equifax has possessed Ms. Kelley's financial history, including her Social Security Number, birthdate, personal addresses, and other sensitive personally identifying information. Plaintiff was a victim of the breach. Since the breach, she has suffered several fraudulent charges

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

to her debit account and credit account, all of which occurred within a forty-eight-hour period. Additionally, she has spent time monitoring and attempting to protect her credit and accounts from the improper use of her PII obtained by unauthorized third parties as a result of the Data Breach.

B. DEFENDANTS

12. Defendant Equifax Inc. is a multi-billion-dollar corporation formed under the laws of the State of Georgia with its corporate headquarters in Atlanta, GA. It provides credit information services to millions of businesses, governmental units, and consumers across the globe. Equifax operates through various subsidiaries and agents, each of which entities acted as agents of Equifax, or in the alternative, in concert with Equifax.

13. Defendant EISL is a Georgia Limited Liability Company with its principal place of business located in Atlanta, GA. EISL is a subsidiary of Equifax, Inc. that operates in concert with, or for the benefit of Equifax, Inc. EISL's responsibilities specifically include collection and reporting of consumer information to financial institutions.

14. Defendants have conducted and continue to conduct business in the District of Colorado.

III. JURISDICTION AND VENUE

15. This Court has jurisdiction under 28 U.S.C. § 1332 because there are

over 100 Class Members, the amount in controversy exceeds $5 million exclusive of interest and costs, and this is a class action in which many members of the proposed classes, on the one hand, and Defendants, on the other, are citizens of different states.

16. The District of Colorado has personal jurisdiction over Defendants because Defendants do business in Colorado and in this district; Defendants advertise in a variety of media throughout the United States, including Colorado; and many of the acts complained of and giving rise to the claims alleged herein occurred in this District. Defendants intentionally avail themselves of the markets within this state to render the exercise of jurisdiction by this Court just and proper.

17. Venue is proper pursuant to 28 U.S.C. Section 1391 because Defendants conduct substantial business in this District, a substantial part of the events and omissions giving rise to the claims alleged herein occurred in this district, and a substantial part of property that is the subject of the action is situated in this district.

IV. FACTUAL ALLEGATIONS

18. Equifax has collected and stored personal and credit information from Class Members, including Plaintiff.

19. Having collected and stored this personal and credit information, Equifax owed a duty to Plaintiff and the Class Members, who entrusted Defendants

with their private information, to use reasonable care to protect their PII from unauthorized access by third parties and to detect and stop data breaches, to comply with laws implemented to preserve the privacy of this information, and to promptly notify Plaintiff and the members of the nationwide Class and Colorado Subclass (defined in paragraphs 35-39, below) if their information was disclosed to an unauthorized third party.

20. Equifax knew or should have known that its failure to meet this duty would cause substantial harm to Plaintiff and the Class, including serious risks of credit harm and identity theft for years to come.

21. As Equifax was well-aware, or reasonably should have been aware, the PII collected, maintained and stored in their systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, including identity theft and fraud. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Prior to May 2017, Equifax had experienced at least three major cybersecurity incidents in which consumers' personal information was compromised and accessed by unauthorized third parties.

22. Despite the frequent public announcements of data breaches of corporate entities, including Experian (another large credit reporting company, and a competitor of Defendants) and Defendants themselves, Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiff and Class Members,

in breach of its duties to Plaintiff and the Class. Given the Company's history of cyberattacks and its reputation as an industry leader in data breach security, Equifax could have and should have invested more money and resources into ensuring the security of its data and the PII.

23. Because Equifax negligently failed to maintain adequate safeguards, unauthorized third parties managed to exploit a weakness in Equifax's US website application to gain access to sensitive data for roughly two months, beginning in mid-May 2017. The information accessed included names, Social Security Numbers, birthdates, addresses, and, in some cases, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personally identifying information for approximately 182,000 U.S. consumers, were accessed.

24. Equifax Inc. and EISL knew, or reasonably should have known, of the vulnerability in their system as early as March 2017. In or about March 2017, Defendants discovered a vulnerability in their U.S. website: Apache Struts CVE-2017-5638. Despite knowing that this system flaw jeopardized the PII of millions of consumers, they failed to implement an effective patch for at least nine weeks, and failed to monitor whether third persons had exploited this known vulnerability to gain access to consumers' PII and whether consumers' PII was secure.

25. The Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

26. Equifax delayed informing Plaintiff, the Class, and the public of the Data Breach. On September 7, 2017, Equifax announced to the public that it had discovered "unauthorized access" to company data, which jeopardized sensitive information for millions of its consumers.

27. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

28. As a direct, proximate, and foreseeable result of Equifax's failure to meet its duty of care, including by failing to maintain adequate security measures and failing to provide adequate notice of the Data Breach, Plaintiff and the Class have suffered and will continue to suffer substantial harm, including inconvenience, distress, injury to their rights to the privacy of their information, increased risk of

fraud, identity theft, financial harm, the costs of monitoring their credit to detect incidences of this, and other losses consistent with the access of their PII by unauthorized sources.

29. Armed with the stolen information, unauthorized third parties now possess keys that unlock consumers' medical histories, bank accounts, employee accounts, and more. Abuse of sensitive credit and personal information can result in considerable harm to victims of security breaches. Criminals who have stolen PII take out loans, mortgage property, open financial accounts and credit cards in a victim's name, obtain government benefits, file fraudulent tax returns, obtain medical services, and provide false information to police during an arrest, all under the victim's name. Furthermore, this valuable information is also sold to others for similar improper purposes.

30. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands, and attempt instead 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. This time has been lost forever and cannot be recaptured. In all manner of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free from having to deal with the consequences of a credit reporting agency's security failures, as is the case here.

31. A breach of this scale requires Plaintiff and Class Members to incur the burden of scrupulously monitoring their financial accounts and credit histories to protect themselves against identity theft and other fraud and to spend time and incur out-of-pocket expenses to protect against such theft. This includes obtaining credit reports, enrolling in credit monitoring services, freezing lines of credit, and more. Where identity theft is detected, Plaintiff and Class Members will incur the burden of correcting their financial records and attempting to correct fraud on their accounts, to the extent that that is even possible. Plaintiff and Class Members will likely spend considerable effort and money for the rest of their lives on monitoring and responding to the repercussions of this cyberattack.

32. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's 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 Plaintiff's 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, 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 attempting to address, 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.

33. Because Equifax has demonstrated an inability to prevent a breach or stop it from continuing even after the breach was detected, Plaintiff and Class Members have an undeniable interest in insuring that their PII, which remains in Equifax's possession, is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

V. CLASS ACTION ALLEGATIONS

34. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23 seeking injunctive and monetary relief for Equifax's systemic failure to safeguard personal information of Plaintiff and Class Members.

A. CLASS DEFINITIONS

35. Plaintiff seeks relief in her individual capacity and as a representative of all others who are similarly situated.

36. The "Class" is defined as all persons residing in the United States whose personal data Equifax collected and stored and whose personal information was placed at risk and/or disclosed in the Data Breach affecting Equifax from May to July 2017.

37. The "Colorado Subclass" is defined as all persons residing in Colorado whose personal data Equifax collected and stored and whose personal information was placed at risk and/or disclosed in the Data Breach affecting Equifax from May to July 2017.

38. Excluded from either class are all attorneys for the class, officers, and members of Equifax, including officers and members of any entity with an ownership interest in Equifax, any judge who sits on this case, and all jurors and alternate jurors who sit on this case.

39. Except where otherwise noted, "Class Members" shall refer to

members of the Nationwide Class and the Colorado Subclass collectively.

40. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity after having had an opportunity to conduct discovery.

B. REQUIREMENTS OF RULE 23(a)

i. Numerosity and Impracticability of Joinder

41. The proposed Class and Subclass are so numerous that joinder of all members is impracticable.

42. Upon information and belief, there are more than 145 million members of the proposed Nationwide Class, and many thousands of members in the Colorado Subclass.

43. The Class Members are readily ascertainable. Equifax has access to information about the Data Breach, the time period of the Data Breach, and which individuals were affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice.

ii. Common Questions of Law and Fact

44. Every Class Member suffered injuries as alleged in this complaint because of Defendants' misconduct. The prosecution of Plaintiff's claims will require the adjudication of numerous questions of law and fact common to the

Classes. The common questions of law and fact predominate over any questions affecting only individual Class Members. The common questions include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants owed a duty to Plaintiff and Class Members to adequately protect their personal information;

c. Whether Defendants breached their duties to protect the personal information of Plaintiff and Class Members;

d. Whether Defendants knew or should have known that Equifax's data security systems and processes were unreasonably vulnerable to attack;

e. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of personal information; and

f. Whether Plaintiff and Class Members are entitled to equitable relief including injunctive relief.

iii. Typicality of Claims and Relief Sought

45. Plaintiff has suffered the same violations and similar injuries as other Class Members arising out of and caused by Defendants' common course of

conduct. All Class Members were subject to the same acts and omissions by Defendants, as alleged herein, resulting in the breach of personal information.

46. Plaintiff possesses and asserts each of the claims on behalf of the proposed Class and Subclass. She seeks similar relief as other Class Members.

iv. Adequacy of Representation

47. Plaintiff's interests are coextensive with those of the members of the proposed Classes. Each suffered risk of loss and credit harm and identity theft caused by Equifax's wrongful conduct and negligent failure to safeguard their data, the injuries suffered by Plaintiff and the Class Members are identical (i.e. the costs to monitor and repair their credit through a third-party service), and Plaintiff's claims for relief are based upon the same legal theories as are the claims of the other Class Members. Plaintiff is willing and able to represent the proposed Class fairly and vigorously.

48. Plaintiff has retained counsel sufficiently qualified, experienced, and able to conduct this litigation and to meet the time and fiscal demands required to litigate a class action of this size and complexity.

C. REQUIREMENTS OF RULE 23(b)(2)

49. Equifax has acted or refused to act on grounds generally applicable to Plaintiff and the proposed Class by failing to take necessary steps to safeguard Plaintiff's and Class Members' personal information.

50. Equifax's systemic conduct justifies the requested injunctive and declaratory relief with respect to the Class.

51. Injunctive, declaratory, and affirmative relief are predominant forms of relief sought in this case. Entitlement to declaratory, injunctive, and affirmative relief flows directly and automatically from proof of Equifax's failure to safeguard consumers' personal information. In turn, entitlement to declaratory, injunctive, and affirmative relief forms the factual and legal predicate for the monetary and non-monetary remedies for individual losses caused by Equifax's failure to secure such information.

D. REQUIREMENTS OF RULE 23(b)(3)

52. The resolution of this case is driven by the common questions set forth above. These questions, relating to Equifax's liability and the Class Members' entitlement to relief, are substantial and predominate over any individualized issues.

53. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. In fact, no other feasible methods exist. Individual class members have modest damages and lack the financial resources to vigorously prosecute a lawsuit against a large corporation such as Equifax.

54. Class action treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously,

efficiently, and without the unnecessary duplication of efforts and expense that numerous individual actions engender.

55. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent and/or varying adjudications with respect to the individual members of the Class, establishing incompatible standards of conduct for Defendants and resulting in the impairment of Class Members' rights and the disposition of their interests through actions to which they were not parties.

56. The issues in this class action can be decided by means of common, class-wide proof. In addition, the Court can, and is empowered to, fashion methods to efficiently manage this action as a class action.

E. RULE 23(c)(4) ISSUE CERTIFICATION

57. Additionally, or in the alternative, the Court may grant "partial" or "issue" certification under Rule 23(c)(4). Resolution of common questions of fact and law would materially advance the litigation for all Class Members.

COUNT I

WILLFUL VIOLATION OF THE FEDERAL FAIR CREDIT REPORTING ACT

(On Behalf of the Nationwide and Colorado Classes against all Defendants)

58. Plaintiff incorporates paragraphs 1 through 57 by reference.

59. Plaintiff and Class Members are consumers entitled to the protections of the Fair Credit Reporting Act, 15 U.S.C. § 1681a(c) ("FCRA").

60. 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).

61. 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.

62. 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).

63. 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.

64. 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 Class Members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

65. Equifax furnished 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.

66. 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.

67. 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.

68. 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 Plaintiff and other members of the Class of their rights under the FCRA.

69. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiff's and the Class Members' PII for no permissible purposes under the FCRA.

70. Plaintiff and the Class Members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiff and each of the 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).

71. Plaintiff and the 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 and Colorado Classes against all Defendants)

72. Plaintiff incorporates paragraphs 1 through 71 by reference.

73. 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.

74. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiff's and Class Members' PII and consumer reports for no permissible purposes under the FCRA.

75. Plaintiff and the Class Members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiff and each of the Class Members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

76. Plaintiff 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 III

VIOLATION OF COLORADO CONSUMER PROTECTION ACT

(On Behalf of the Colorado Class against all Defendants)

77. Plaintiff incorporates paragraphs 1 through 76 by reference.

78. While operating in Colorado, Equifax committed deceptive act and practices in the conduct of business, trade, and commerce in violation of Colo. Rev. Stat. Ann. § 6-1-101 *et seq*. These acts and practices include, but are not limited to:

a. Equifax failed to enact adequate privacy and security measures to protect the Plaintiff's and the Colorado Subclass Members' PII from unauthorized disclosure, release, data breach, and theft, which was a direct and proximate cause of the Data Breach;

b. Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Colorado Subclass Members' PII from

unauthorized disclosure, release, data breach, and theft in violation of Colo. Rev. Stat. Ann. § 6-1-105(1)(e), (g), and (u);

d. Equifax knowingly omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for Plaintiff's and the Colorado Subclass Members' PII, in violation of Colo. Rev. Stat. Ann § 6-1-105(1)(e), (g), and (u), and as a result of the omission, suppression, or concealment, Plaintiff and Colorado Subclass Members were misled into thinking that their PII was secure;

e. Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Colorado Subclass Members' PII, including but not limited to duties imposed by the FCRA, 15 U.S.C. § 1681e, and GLBA, 15 U.S.C. § 6801 *et seq*;

f. Equifax failed to maintain the privacy and security of the Colorado Subclass Members' PII, in violation of duties imposed by applicable federal and state laws, including, but not limited to, those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach;

79. As a direct and proximate result of Defendants' practices, Plaintiff and the Colorado Subclass Members suffered injuries, as described above, including, but not limited to, fraudulent charges on accounts, time and expenses related to monitoring their financial accounts for fraudulent activity, and increased, imminent risk of fraud and identity theft, and loss of the confidentiality, privacy, and value of their PII.

80. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and the Colorado Subclass Members' PII and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were therefore negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Colorado Subclass Members.

81. Plaintiff, individually and on behalf of the Colorado Subclass, seeks monetary relief against Defendants measured as the greater of a) actual damages in an amount to be determined at trial and discretionary trebling of such damages, or b) statutory damages in the amount of $500 for each Plaintiff and Colorado Subclass member, consistent with Colo. Rev. Stat. Ann. § 6-1-113.

82. Plaintiff also seeks an order enjoining Defendants' unfair, unlawful, and/or deceptive practices, declaratory relief, attorneys' fees, and other just and proper relief available under Colo. Rev. Stat. Ann. § 6-1-101 *et. seq.*

COUNT IV

NEGLIGENCE

(On Behalf of the Nationwide and Colorado Classes against all Defendants)

83. Plaintiff incorporates paragraphs 1 through 82 by reference.

84. Equifax owed a duty to Plaintiff and Class Members to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class Members' information was adequately secured from unauthorized access.

85. Equifax owed a duty to Plaintiff and Class Members to implement intrusion detection processes that would detect a data breach in a timely manner.

86. Equifax also had a duty to delete any PII that was no longer needed to serve client needs.

87. Equifax owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Class Members' PII.

88. Equifax also had independent duties under state laws that required Equifax to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the Data Breach.

89. Equifax had a special relationship with Plaintiff and Class Members because the Plaintiff and Class Members entrusted Equifax with their PII. This

provided an independent duty of care. Moreover, Equifax had the ability to protect its systems and the PII it stored on them from attack.

90. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class Members' PII; (b) failing to detect and end the Data Breach in a timely manner; (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII; and (d) failing to provide adequate and timely notice of the breach.

91. Because of Equifax's breach of its duties, Class Members' PII has been accessed by unauthorized individuals.

92. Plaintiff and Class Members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security systems would cause damages to Class Members.

93. Equifax engaged in this misconduct recklessly, in conscious neglect of duty and in callous indifference to consequences, and, in the alternative, with such want of care as would raise a presumption of a conscious indifference to consequences. Equifax was, or should reasonably have been, aware of its misconduct and of the foreseeable injury that would probably result, and with reckless indifference to consequences, consciously and intentionally committed the

wrongful acts and omissions herein. Equifax's actions and omissions were, therefore, not just negligent, but grossly negligent, reckless, willful, and wanton.

94. As a result of Equifax's negligence, Plaintiff and/or Class Members suffered and will continue to suffer injury, which includes, but is not limited to, the monetary difference between the amount paid for services as promised and the services actually provided by Defendants (which did not include adequate or industry standard data protection), inconvenience and exposure to a heightened, and/or imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII has also diminished the value of the PII. Plaintiff and the Class Members have also experienced other damages consistent with the theft of their PII. Through its failure to timely discover and provide clear notification of the Data Breach to consumers, Equifax prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

95. The damages to Plaintiff and the Class Members were a direct, proximate, reasonably foreseeable result of Equifax's breaches of its duties.

96. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT V

NEGLIGENCE PER SE

(On Behalf of the Nationwide and Colorado Classes against all Defendants)

97. Plaintiff incorporates paragraphs 1 through 96 by reference.

98. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect PII.

99. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. 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, including, specifically, the immense damages that would result to Plaintiff and Class Members.

100. Equifax's violation of Section 5 of the FTC Act constitutes negligence per se.

101. Equifax also violated the FCRA, as stated in Counts I and II. Equifax's violation of the FCRA constitutes negligence per se.

102. The Gramm-Leach-Bliley Act ("GLBA") requires covered entities to satisfy certain standards relating to administrative, technical, and physical safeguards:

> (1) to insure the security and confidentiality of customer records and information;
>
> (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
>
> (3) 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).

103. Businesses subject to the GLBA "should take preventative measures to safeguard customer information against attempts to gain unauthorized access to the information." Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F.

104. In order to satisfy their obligations under the GLBA, Equifax was 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. § 314.3; *see also* Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F. (Subject companies must "design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the […] company's activities"). This obligation included considering and, where the Company determined appropriate, adopting mechanisms for "[e]ncryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access." *Id.*

105. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax 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.* "The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities." *Id.*

106. Equifax had an "affirmative duty to protect their customers' information against unauthorized access or use." *Id.* Timely notification of customers in the event of a data breach is key to meeting this affirmative obligation. Accordingly, when Equifax 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.* Sensitive customer information includes much of the PII released in the Data Breach.

107. Equifax violated by 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, Equifax's failure to implement and maintain adequate data security practices to safeguard Class Members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII.

108. Equifax also violated the GLBA by failing to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information.

109. To the extent that Equifax is not subject to title V of the GLBA, it also violated Colo. Rev. Stat. Ann. § 6-2-716 which requires a business to disclose such breach either "in the most expedient time possible and without unreasonable delay" (if the business owns or licenses the computerized data), Colo. Rev. Stat. Ann. § 6-

2-716(2)(a), or "immediately following discovery" (if the business does not own the computerized data). Colo. Rev. Stat. Ann. § 6-2-716(2)(b).

110. Defendants violated the Colo. Rev. Stat. Ann. § 6-2-716 by failing to conduct an adequate investigation to identify the breach, failing to promptly determine whether there had been a breach, and failing to notify Plaintiff and Class Members of the breach in the most expedient manner possible. Defendants failed to discover the breach for over two months. They then waited over a month to notify Plaintiff and Class Members that any breach had occurred.

111. Plaintiff and Class Members are within the class of persons that the FTC Act, the FCRA, the GLBA, and (to the extent title V of the GLBA does not apply) Colo. Rev. Stat. Ann. § 6-2-716 were intended to protect.

112. The FTCA, the FRCA, the GLBA, and Colo. Rev. Stat. Ann. § 6-2-716 establish statutory standards of care, which Equifax has inexcusably violated. These inexcusable violations constitute negligence per se.

113. Plaintiff and Class Members were foreseeable victims of Equifax's violation of the FTC Act, the FCRA, the GLBA, and (to the extent title V of the GLBA does not apply) Colo. Rev. Stat. Ann. § 6-2-716. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately report it to Class Members themselves would cause damages to Class Members.

114. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act, the FCRA, the GLBA, and (to the extent title V of the GLBA does not apply) Colo. Rev. Stat. Ann. § 6-2-716 were 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 Plaintiff and the Class.

115. Equifax engaged in this misconduct recklessly, in conscious neglect of duty and in callous indifference to consequences, and, in the alternative, with such want of care as would raise a presumption of a conscious indifference to consequences. Equifax was, or should reasonably have been, aware of its misconduct and of the foreseeable injury that would probably result, and with reckless indifference to consequences, consciously and intentionally committed the wrongful acts and omissions herein. Equifax's actions and omissions were, therefore, not just negligent, but grossly negligent, reckless, willful, and wanton.

116. As a direct and proximate result of Equifax's negligence per se, Plaintiff and/or Class Members suffered and will continue to suffer injury, which includes, but is not limited to, the monetary difference between the amount paid for services as promised and the services actually provided by Defendants (which did not include adequate or industry standard data protection), inconvenience and

exposure to a heightened, and/or imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII has also diminished the value of the PII. Plaintiff and Class Members have also experienced other damages consistent with the theft of their PII. Through its failure to timely discover and provide clear notification of the Data Breach to consumers, Equifax prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

117. But for Equifax's violation of the applicable laws and regulations, Class Members' PII would not have been accessed by unauthorized individuals.

118. The damages to Plaintiff and the Class Members were a direct, proximate, reasonably foreseeable result of Equifax's breaches of the applicable laws and regulations.

119. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT VI

UNJUST ENRICHMENT

(On Behalf of the Nationwide and Colorado Classes against all Defendants)

120. Plaintiff incorporates paragraphs 1 through 119 by reference.

121. Equifax received payment to perform services that included protecting Plaintiff's and the Class Members' PII. Equifax failed to do this, but retained Plaintiff's and the Class Members' payments.

122. Equifax retained the benefit of said payments under circumstances which renders it inequitable and unjust for it to retain such benefits without paying for their value.

123. Defendants have knowledge of said benefits.

124. Plaintiff and Class Members are entitled to recover damages in an amount to be proven at trial.

COUNT VII

DECLARATORY JUDGMENT

(On Behalf of the Nationwide and Colorado Classes against all Defendants)

125. Plaintiff incorporates paragraphs 1 through 124 by reference.

126. Equifax owes duties of care to Plaintiff and Class Members that require it to adequately secure PII.

127. Equifax still possesses PII pertaining to Plaintiff and Class Members.

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

129. Accordingly, Equifax has not satisfied its contractual obligations and legal duties to Plaintiff 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.

130. Equifax's violations of its obligations to Plaintiff and Class Members have caused them actual harm.

131. Plaintiff, 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, 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 Equifax's systems on a periodic basis, and ordering Equifax 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 PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

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

f. conducting regular database scanning and securing checks;

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; and

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

PRAYER FOR RELIEF ON INDIVIDUAL AND CLASS ACTION CLAIMS

WHEREFORE, the Plaintiff and Class Representative, on her own behalf and on behalf of the Class, prays that this Court:

(1) Certify this case as a class action maintainable under Federal Rules of Civil Procedure Rule 23, on behalf of the proposed Class and Subclass;

designate the Plaintiff as Class Representative; and designate Plaintiff's counsel of record as Class Counsel;

(2) Declare and adjudge that Defendants' policies, practices, and procedures challenged herein are illegal and in violation of the rights of the Plaintiff and Class Members;

(3) Issue a permanent injunction against Defendants and their partners, officers, trustees, owners, employees, agents, attorneys, successors, assigns, representatives, and any and all persons acting in concert with them from engaging in any conduct violating the rights of Plaintiff, members of the Class, and those similarly situated to them;

(4) Order injunctive relief requiring Defendants to (a) strengthen their data security systems that maintain PII to comply with the applicable state laws alleged herein and best practices under industry standards; (b) engage third-party auditors and internal personnel to conduct security testing and audits on Defendants' systems on a periodic basis; (c) promptly correct any problems or issues detected by such audits and testing; and (d) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

(5) Award compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement to Plaintiff and Class Members in an amount to be determined at trial;

(6) Order Defendants to make the Plaintiff and Class Members whole by providing them with any other monetary and affirmative relief;

(7) Order Defendants to pay all costs associated with Class notice and administration of Class-wide relief;

(8) Award Plaintiff and the Class their litigation costs and expenses, including, but not limited to, reasonable attorneys' fees;

(9) Award Plaintiff and Class Members all pre-judgment interest and post-judgment interest available under law;

(10) Award Plaintiff and Class Members any other appropriate equitable relief;

(11) Order that this Court retain jurisdiction of this action until such time as the Court is satisfied that the Defendants have remedied the practices complained of herein and are determined to be in full compliance with the law; and

(12) Award additional and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff demands a trial by jury on all issues triable of right by jury.

/s/ Kevin Sharp

Kevin Sharp (TN SBN 016287)
SANFORD HEISLER SHARP, LLP
611 Commerce St., Suite 3100
Nashville, TN 37203
Telephone: (615) 434-7001
Facsimile: (615) 434-7020
ksharp@sanfordheisler.com

Attorney for Plaintiff and the Class

JS 44 (Rev. 06/17)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

Melissa Kelley, on behalf of herself and all others similarly situated

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

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

Kevin Sharp, Sanford Heisler Sharp, LLP, 611 Commerce Street, Suite 3100, Nashville, TN 37203, (615) 434-7001

DEFENDANTS

Equifax Inc. and Equifax Information Services, LLC

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.

Attorneys *(If Known)*

Sidney Stewart Haskings, King & Spalding, 1180 Peachtree Street Atlanta, GA 30309, (404) 572-4687

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

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

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

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

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

Click here for: Nature of Suit Code Descriptions.

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

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

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

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

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

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

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

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

- ❒ 625 Drug Related Seizure of Property 21 USC 881
- ❒ 690 Other

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

- ❒ 462 Naturalization Application
- ❒ 465 Other Immigration Actions

- ❒ 422 Appeal 28 USC 158
- ❒ 423 Withdrawal 28 USC 157

- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 835 Patent - Abbreviated New Drug Application
- ❒ 840 Trademark

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

- ❒ 870 Taxes (U.S. Plaintiff or Defendant)
- ❒ 871 IRS—Third Party 26 USC 7609

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

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
15 U.S.C. 1681 et seq.

Brief description of cause:
Violation of Fair Credit Reporting Act, Negligence, Contract Claims and Others

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE Judge Thomas W. Thrash DOCKET NUMBER 1:17-md-2800-TWT

DATE
01/26/2018

SIGNATURE OF ATTORNEY OF RECORD
s/ Kevin Sharp

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE