THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

MELISSA DERBY, on behalf of herself and all others similarly situated, Plaintiff, v. EQUIFAX, INC., a Georgia corporation, Defendant.	**CASE NO.: _____** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Melissa Derby ("Plaintiff"), on behalf of herself and all others similarly situated, alleges, based upon her personal information and the investigation of her counsel, as follows:

NATURE OF THE CASE

1. This is a data breach class action on behalf of some 143 million consumers whose personal identifying information ("PII") including dates of birth, names, addresses, Social Security numbers ("SSNs"), driver's license numbers, and other personal information (collectively, "Data") was taken in a cyber-attack from Defendant Equifax, Inc. ("Equifax").

2. Equifax failed to adequately safeguard consumers' PII because it lacked proper safeguards to maintain security of Plaintiff's and Class Members' personal information. Equifax's lack of reasonable security provided a means for unauthorized intruders to access Equifax's computer network and steal consumers' sensitive PII.

3. According to Equifax's September 7, 2017 announcement of the data breach, the breach occurred "from mid-May through July 2017" and compromised data included "names, Social

Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, 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, were accessed."[1]

4. Despite the fact that around 143 million customers had PII that was accessed as a result of the breach, according to their September 7, 2017 announcement, Equifax is only planning to "send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted."[2] This constitutes less than 3% of those affected by the breach.

5. In its September 7, 2017 announcement, Equifax indicated that it had "established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection."[3] Plaintiff visited Equifax's website on September 8, 2017 and was informed that "we believe that your personal information may have been impacted by this incident."

6. Armed with the sensitive information obtained through the breach, data thieves can incur fraudulent debts; open new financial or utility accounts in a victim's name; use the victim's information to obtain government benefits; file fraudulent tax return using the victim's information to obtain a tax refund; obtain a driver's license or identification card in the victim's name but with another person's picture; and give false information to police during an arrest, amongst other things.

7. As a result of the breach, Plaintiff and members of the Class (as defined below) are exposed to a heightened and imminent risk of fraud and identity theft and must now closely monitor their financial accounts to guard against identity theft well into the future. As a result, Plaintiff and

[1] https://www.equifaxsecurity2017.com/ (last visited September 8, 2017).
[2] *Id.*
[3] *Id.*

Class Members may be faced with fraudulent debt, incur out of pocket costs for, among other things, obtaining credit reports, credit freezes, or other protective measures to deter and detect identity theft.

8. Plaintiff seeks to remedy these harms on behalf of herself and all similarly-situated individuals whose personal information was accessed during the breach.

9. Plaintiff seeks remedies including but not limited to statutory damages under the Fair Credit Reporting Act ("FCRA"), reimbursement of out-of-pocket losses, further credit monitoring services with accompanying identity theft insurance, and improved data security.

PARTIES

10. Plaintiff Melissa Derby is a resident of Pittsburgh, Pennsylvania.

11. Ms. Derby visited Equifax's website on September 8, 2017 to learn more about the data breach. The "Schedule. Enroll. Activate." section of the equifaxsecurity2017.com website states that "[t]o enroll and activate your complimentary identity theft protection and credit file monitoring product, called TrustedID Premier, please follow the steps outlined below. At the beginning of this process, you will find out whether your personal information may have been impacted by this incident." It noted that customers would "be asked to provide your last name and the last six digits of your Social Security number" and "[b]ased on that information, you will receive a message indicating whether your personal information may have been impacted by this incident."[4]

12. Ms. Derby followed the instructions set forth on the equifaxsecurity2017.com website, entering her last name and portions of her Social Security number. In response, she received a message indicating "[b]ased on the information provided, we believe that your personal information may have been impacted by this incident. Click the button below to continue your enrollment in TrustedID Premier."

[4] https://www.equifaxsecurity2017.com/enroll/ (last visited September 8, 2017).

13. Defendant Equifax is a Georgia corporation whose principal office address is 1550 Peachtree Street NW, Atlanta, GA, 30309-2402. Defendant is a credit reporting agency.

JURISDICTION AND VENUE

14. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because claims are brought under the federal Fair Credit Reporting Act, 15 U.S.C. §§ 1681e, *et seq*.

15. This Court has diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000 exclusive of interest and costs, and Plaintiff and many members of the class are citizens of states different from Defendant.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Plaintiff Derby and some of the class members reside in this District. Their causes of action arose, in part, in this District.

FACTS

Equifax – Data Protection, Management and Customer Support Experts

17. Defendant Equifax is a credit reporting agency that touts itself as "a global information solutions company that uses trusted unique data, innovative analytics, technology and industry expertise to power organizations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions."[5]

18. According to Equifax's Chairman and Chief Executive Officer, Richard F. Smith, the company prides itself "on being a leader in managing and protecting data." He further indicated that

[5] https://www.equifaxsecurity2017.com/ (last visited September 8, 2017).

Equifax is "focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."[6]

19. Equifax's website also indicates that its "data assets, technology and analytics transform knowledge into insights that power better decisions. This knowledge enables our customers to make better business decisions and consumers to progress towards a better life. We serve as a consumer advocate, steward of financial literacy, and champion of economic advancement."[7]

20. On that website, Mr. Smith is quoted as saying "Equifax helps people make better decisions by weaving unique data and insights into knowledge that makes a difference. Our strategic focus has stood the test of time and allowed us to evolve into a better, more sophisticated partner for our customers, consumers, and shareholders. No longer just a consumer credit company, we are a global insights powerhouse driven by innovation, adherence to our core values, and the best talent in the industry."[8]

21. Despite Equifax's professed expertise in the area of data protection, management and customer support, its lapse in security permitting the breach and its response to this breach has been inadequate. Equifax states that the data breach occurred as a resulted of a "website application vulnerability" that was "exploited" and permitted access, among other things, to "names Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers."[9] Equifax states it will only notify less than 3% of the 143 million people who are victims of this data breach that their information has been accessed, leaving everyone else to have to take actions to try to find out if they are a victim. Once someone figures out if they are a victim of this data breach, all Equifax

[6] *Id.*
[7] http://www.equifax.com/about-equifax/ (last accessed September 8, 2017).
[8] *Id.*
[9] *Id.*

has offered them to date is the opportunity to sign up for a "credit file monitoring and identity theft protection" called TrustedID Premier, which "includes 3-Bureau credit monitoring of Equifax, Equifax and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers – all complimentary to U.S. consumers for one year."[10] Understandably, Plaintiff and Class members may have doubts regarding this credit monitoring, given its failure to prevent the data breach herein. In any event, providing one year of credit monitoring is woefully insufficient to redress the heightened and imminent risks of identity theft created by Equifax's data breach.

22. Despite the fact that Equifax failed to notify the public until September 7, 2017 and offers woefully insufficient relief to its data breach victims, several Equifax executives took the opportunity to ensure their own profit by selling shares of the company valued at nearly $1.8 million just days after the Company detected the breach in late July 2017 and weeks before it made the breach public and its stock price dropped as a result.[11]

Equifax – The Data Breach

23. On July 29, 2017, Equifax purportedly discovered that one or more unauthorized persons accessed data housed on its servers.[12]

24. On September 7, 2017, Equifax "announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017."[13]

---

[10] https://www.equifaxsecurity2017.com/ (last visited September 8, 2017).
[11] https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack (last accessed September 8, 2017).
[12] *Id.*
[13] *Id.*

25. Equifax's September 7, 2017 announcement also indicated that it "has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases."[14]

26. According to Equifax's September 7, 2017 announcement of the data breach, the compromised data included "names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, 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, were accessed."[15]

27. In response to the breach, "Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection," as described *supra*.[16]

28. According to their September 7, 2017 announcement, Equifax is only planning to "send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted."[17]

Equifax – Past Data Breaches

29. Equifax has experienced data breaches in the past, as detailed in an article by Thomas Fox-Brewster on forbes.com entitled "A Brief History of Equifax Security Fails."[18] That article mentioned various data breaches at Equifax over the past few years, including:

> •A class action lawsuit which was filed regarding "a May 2016 incident in which Equifax's W-2 Express website had suffered an attack that resulted in the leak of 430,000 names, addresses, social security numbers and other personal information of retail firm Kroger.

[14] *Id.*
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#6495a79c677c (last accessed September 8, 2017).

> Lawyers for the class action plaintiffs argued Equifax had 'wilfully ignored known weaknesses in its data security, including prior hacks into its information systems.'… In the end, the case was dropped without prejudice (i.e. the claims could be brought again), with the stipulation that Equifax fix a glaring security issue" regarding PIN numbers.
>
> •However, "problems with PINs appeared to have continued after that settlement in September last year. As independent cybersecurity reporter Brian Krebs reported in May 2017 an Equifax note to customers that hackers had used personal information to guess personal questions of employees in order to reset the 4-digit PIN given and stolen tax data. In its disclosure, Equifax said the unauthorized access to the information occurred between April 17 2016 and March 29 the following year."
>
> •Additionally, "[i]n January 2017, Equifax was forced to confess to a data leak in which credit information of a 'small number' of customers at partner LifeLock had been exposed to another user of the latter's online portal."
>
> •Finally, "Equifax reported to the New Hampshire attorney general of a breach, admitting that between April 2013 and January 2014, an 'IP address operator was able to obtain the credit reports using sufficient personal information to meet Equifax's identity verification process.' There were other smaller data leaks reported by Equifax to the AG, though they only appeared to affect a handful of people."[19]

30. That article also noted that there are serious questions about Equifax's security procedures, at least one of which was raised even before the latest data breach. It further noted that "[t]he good-guy hackers have found myriad old technologies running the Equifax site, many of which could be vulnerable to cyberattack. Researcher Kenneth White discovered a link in the source code on the Equifax consumer sign-in page that pointed to Netscape, a web browser that was discontinued in 2008. Kevin Beaumont, a British security pro who's spent 17 years helping protect businesses, found decade-old software in use."[20]

31. Equifax, by virtue of its alleged expertise and own past data breaches, was or should have been well aware of the risk of data breaches of its own databases, and should have taken

[19] *Id.*
[20] *Id.*

reasonable steps to prevent the data breach in the first place, or to detect the data breach sooner than it did.

CLASS ACTION ALLEGATIONS

32. Plaintiff brings this action on behalf of a Class pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), (b)(3), and (c)(4), on behalf of all persons in the United States whose personal information was accessed by unauthorized individuals in Equifax's data breach announced on September 7, 2017.[21]

33. Excluded from the Class are: (i) Equifax, including any entity in which Equifax has a controlling interest, is a parent or subsidiary, or which is controlled by Equifax, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Equifax; and (ii) the judges to whom this action is assigned and any members of their immediate families.

34. The members of the Class are so numerous that joinder of all members is impracticable. The class includes approximately 143 million individuals whose personal information was compromised by the data breach. Class Members can be identified by the records retained by Equifax.

35. There are various questions of law and fact common to Plaintiff and the Class, including but not limited to the following:

- Whether Equifax engaged in the wrongful conduct alleged herein;
- Whether Equifax owed a duty to Plaintiff and Class Members to adequately protect their PII;
- Whether Equifax owed a duty to Plaintiff and Class Members to provide timely and accurate notice of the data breach;

[21] Alternatively, if the Court does not certify a nationwide class for some or all of her claims, Plaintiff seeks a multistate or state-wide class, including Pennsylvania.

- Whether Equifax negligently failed to implement and maintain commercially reasonable procedures to ensure the security of Plaintiff's and Class Members' PII;
- Whether Equifax breached its duties to Plaintiff and Class Members to adequately protect their PII;
- Whether Equifax breached its duties to Plaintiff and Class Members to timely and accurately provide notice of the data breach;
- Whether Equifax knew or should have known that its computer systems were vulnerable to cyber-attack;
- Whether Equifax's conduct, including its failure to act, was the proximate cause of the data breach;
- Whether Equifax's actions and/or failures to act were the proximate cause of harm to Plaintiff and Class Members;
- Whether Plaintiff and Class Members suffered injury as a result of Equifax's conduct or failure to act; and
- Whether Plaintiff and Class Members are entitled to damages, restitution, and/or equitable relief.

36. Plaintiff's claims are typical of the claims of the Class. Plaintiff's PII was compromised by the data breach announced by Equifax on September 7, 2017. Therefore, Plaintiff is no different in any material respect from any other members of the Class, and the relief sought by Plaintiff is common to the relief sought by the Class.

37. Plaintiff is an adequate representatives of the Class because her interests are neither antagonistic to, nor in conflict with, the interests of Class Members she seeks to represent, and she has retained counsel competent and experienced in conducting complex class action litigation. Plaintiff and her counsel will adequately protect the interests of the Class.

38. A class action is superior to other available means for the fair and efficient adjudication of this dispute. Plaintiff and Class Members have been harmed by Equifax's actions and

inactions. The damages suffered by each individual Class Member are relatively small while the burden and monetary expense needed to individually prosecute this case against Equifax is substantial. Thus, it would be virtually impossible for Class Members individually to redress effectively the wrongs done to them. Absent a class action, Equifax will retain the benefits of its wrongdoing despite its serious violations of the law. Moreover, even if members of the Class could afford individual actions, a multitude of such individual actions still would not be preferable to class wide litigation. Individual actions also present the potential for inconsistent or contradictory judgments, which would be dispositive of at least some of the issues and hence interests of the other members not party to the individual actions, would substantially impair or impede their ability to protect their interests, and would establish incompatible standards of conduct for the party opposing the class.

39. By contrast, a class action presents far fewer litigation management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Also, or in the alternative, the Class may be certified because Equifax has acted or refused to act on grounds generally applicable to the Class, thereby making preliminary and final injunctive relief and corresponding declaratory relief appropriate. Also in the alternative, the Class may be certified with respect to particular issues.

FIRST CAUSE OF ACTION
Willful Violation of the Fair Credit Reporting Act (on Behalf of Plaintiff and the Class)

40. Plaintiff hereby incorporates the foregoing paragraphs of this Complaint and restates them as if they were fully written herein.

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

42. 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).

43. Equifax is a consumer reporting agency under the FCRA because it, for monetary fees, 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.

44. 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).

45. 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).

46. The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Plaintiff and 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 Plaintiff and Class Members' eligibility for credit.

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

48. Equifax furnished the Plaintiff and 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.

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

50. Equifax willfully 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 nature of Equifax's violations is supported by, among other things, Equifax's other data breaches in the past. Further, Equifax touts itself as an industry leader in managing and protecting data; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

51. Equifax also acted willfully 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 Class Members of their rights under the FCRA.

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

53. Plaintiff and the Class Members have been damaged by Equifax's willful 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) (emphasis added).

54. 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)

SECOND CAUSE OF ACTION

Negligent Violation of the Fair Credit Reporting Act (on Behalf of Plaintiff and the Class)

55. Plaintiff hereby incorporates the foregoing paragraphs of this Complaint and restates them as if they were fully written herein.

56. 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, Equifax's other data breaches in the past. Further, as an enterprise claiming to be an industry leader in managing and protecting data, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

57. 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.

58. 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).

59. Plaintiff and 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).

THIRD CAUSE OF ACTION
Negligence (on Behalf of Plaintiff and the Class)

60. Plaintiff hereby incorporates the foregoing paragraphs of this Complaint and restates them as if they were fully written herein.

61. Equifax owed a duty to Plaintiff and Class Members, arising from the sensitivity of the information and the foreseeability of its data safety shortcomings resulting in an intrusion, 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 Plaintiff and Class Members' information was adequately secured from unauthorized access.

62. Equifax's privacy policy acknowledged Equifax's duty to adequately protect Plaintiff and Class Members' PII. Specifically, it states, "We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."[22]

63. Equifax owed a duty to Class members to implement intrusion detection processes that would detect a data breach in a timely manner.

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

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

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

67. Equifax had a special relationship with Plaintiff and Class Members from being entrusted with their PII, which provided an independent duty of care. Plaintiff's and other Class Members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, Equifax had the ability to protect its systems and the PII it stored on them from attack.

68. Equifax's role to utilize and purportedly safeguard Plaintiff's and Class Members' PII presents unique circumstances requiring a reallocation of risk.

---

[22] http://www.equifax.com/privacy/ (last accessed September 8, 2017).

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

70. Specifically, by their own admission, Equifax discovered the breach on July 29, 2017,[23] but did not publicly announce the breach until September 7, 2017.[24]

71. Furthermore, despite the fact that around 143 million customers had PII that was accessed as a result of the breach, according to their September 7, 2017 announcement and the fact that Equifax has the names, addresses and emails for most or all of those customers, Equifax is only planning to "send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted."[25] This constitutes less than 3% of those affected by the breach.

72. Equifax also failed to notify affected customers in accordance with the Pennsylvania Breach of Personal Information Notification Act, 73 P.S. § 2301 *et seq.*

73. But for Equifax's breach of its duties, Class Members' PII would not have been accessed by unauthorized individuals.

---

[23] Despite the fact that Equifax failed to notify the public until September 7, 2017, several Equifax executives sold shares of the company valued at nearly $1.8 million just days after the Company detected the breach. https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack (last accessed September 8, 2017).

[24] https://www.equifaxsecurity2017.com/ (last visited September 8, 2017).

[25] *Id.*

74. 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 Plaintiff and Class Members.

75. 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.

76. As a result of Equifax's willful failure to prevent the Data Breach, Plaintiff and Class Members suffered injury, which includes but is not limited to exposure to a heightened, 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 Member's PII has also diminished the value of the PII.

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

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

FOURTH CAUSE OF ACTION
Negligence Per Se (On behalf of Plaintiff and the Class)

79. Plaintiff hereby incorporates the foregoing paragraphs of this Complaint and restates them as if they were fully written herein.

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

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

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

83. Equifax also failed to notify affected customers in accordance with the Pennsylvania Breach of Personal Information Notification Act, 73 P.S. § 2301 *et seq.*

84. Defendant's failure to comply with the applicable laws and regulations constitutes negligence *per se.*

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

86. As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiff and Class Members suffered injury, which includes but is not limited to exposure to a heightened, 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.

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

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

FIFTH CAUSE OF ACTION
Constructive Fraud (On behalf of Plaintiff and the Class)

89. Plaintiff hereby incorporates the foregoing paragraphs of this Complaint and restates them as if they were fully written herein.

90. Equifax owed a duty to Plaintiff and Class Members to adequately protect their PII under various state and federal laws and regulations by virtue of being a consumer reporting agency.

91. As a consumer reporting agency to whom Plaintiff's and Class Members' most intimate, sensitive and private personal information and PII was provided, Equifax enjoyed a special relationship of trust and confidence with Plaintiff and Class Members and owed them a heightened duty above and beyond normal commercial relations. Accordingly, Plaintiff and Class Members reasonably expected Equifax would adhere to its obligations to adequately protect the sensitive, personal information they provided including the PII Equifax allowed to be stolen.

92. Equifax breached this duty by failing to maintain security adequate to protect Plaintiff's and Class Members' PII, and by failing to timely and adequately notify them of the breach.

93. As a result of Equifax's conduct, Plaintiff and Class Members are entitled to damages and equitable relief.

PRAYER

Plaintiff, on behalf of herself and Class Members, requests that the Court order the following relief and enter judgment against Equifax as follows:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff Melissa Derby is a proper representative of the Class;

B. Injunctive relief requiring Defendant to (1) strengthen its data security systems that maintain PII to comply with the FCRA, any other applicable law and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendant's systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

C. An order requiring Defendant to pay all costs associated with Class notice and administration of Class-wide relief;

D. An award to Plaintiff and all Class Members of compensatory, consequential, incidental, statutory and punitive damages, restitution, and disgorgement, in an amount to be determined at trial;

E. An award to Plaintiff and all Class Members of additional credit monitoring and identity theft protection services beyond the package Equifax is currently offering;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An order Requiring Defendants to pay pre-judgment and post-judgment interest, as provided by law or equity; and

H. Such other or further relief as the Court may allow.

I.

DATED: September 8, 2017

Respectfully Submitted,

s/ Joseph N. Kravec, Jr.
Joseph N. Kravec, Jr. (PA ID # 68992)

Wyatt A. Lison (PA ID # 90030)
FEINSTEIN DOYLE
PAYNE & KRAVEC, LLC
Law & Finance Building, Suite 1300
429 Fourth Avenue
Pittsburgh, PA 15219-1639
Tel.: (412) 281-8400
Fax: (412) 281-1007
Email: jkravec@fdpklaw.com
wlison@fdpklaw.com

ATTORNEYS FOR PLAINTIFF AND THE PROPOSED 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 DERBY, on behalf of herself and all others similarly situated,

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Feinstein Doyle Payne & Kravec, LLC
429 Fourth Avenue, Suite 1300, Law & Finance Building
Pittsburgh, PA 15219 (412) 281-8400

DEFENDANTS

EQUIFAX, INC., a Georgia corporation,

County of Residence of First Listed Defendant Fulton
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

Attorneys *(If Known)*

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

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

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

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

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

Click here for: Nature of Suit Code Descriptions.

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

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

TORTS

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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

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

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

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

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
28 U.S.C. §1331; 15 U.S.C. §1681e, et seq.

Brief description of cause:
Failure to Maintain Reasonable Procedures

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 09/08/2017

SIGNATURE OF ATTORNEY OF RECORD s/ Joseph N. Kravec, Jr.

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG JUDGE _____

JS 44A REVISED June, 2009
IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF PENNSYLVANIA
THIS CASE DESIGNATION SHEET MUST BE COMPLETED

PART A

This case belongs on the (○ Erie ○ Johnstown ◉ Pittsburgh) calendar.

1. **ERIE CALENDAR** - If cause of action arose in the counties of Crawford, Elk, Erie, Forest, McKean. Venang or Warren, OR any plaintiff or defendant resides in one of said counties.

2. **JOHNSTOWN CALENDAR** - If cause of action arose in the counties of Bedford, Blair, Cambria, Clearfield or Somerset OR any plaintiff or defendant resides in one of said counties.

3. Complete if on **ERIE CALENDAR**: I certify that the cause of action arose in_____ County and that the _____ resides in _____ County.

4. Complete if on **JOHNSTOWN CALENDAR**: I certify that the cause of action arose in _____ County and that the _____ resides in _____ County.

PART B (You are to check ONE of the following)

1. ○ This case is related to Number_____ . Short Caption_____
2. ◉ This case is not related to a pending or terminated case.

DEFINITIONS OF RELATED CASES:

CIVIL: Civil cases are deemed related when a case filed relates to property included in another suit or involves the same issues of fact or it grows out of the same transactions as another suit or involves the validity or infringement of a patent involved in another suit EMINENT DOMAIN: Cases in contiguous closely located groups and in common ownership groups which will lend themselves to consolidation for trial shall be deemed related.
HABEAS CORPUS & CIVIL RIGHTS: All habeas corpus petitions filed by the same individual shall be deemed related. All pro se Civil Rights actions by the same individual shall be deemed related.

PARTC

I. CIVIL CATEGORY (Select the applicable category).

1. ○ Antitrust and Securities Act Cases
2. ○ Labor-Management Relations
3. ○ Habeas corpus
4. ○ Civil Rights
5. ○ Patent, Copyright, and Trademark
6. ○ Eminent Domain
7. ◉ All other federal question cases
8. ○ All personal and property damage tort cases, including maritime, FELA, Jones Act, Motor vehicle, products liability, assault, defamation, malicious prosecution, and false arrest
9. ○ Insurance indemnity, contract and other diversity cases.
10. ○ Government Collection Cases (shall include HEW Student Loans (Education), V A Overpayment, Overpayment of Social Security, Enlistment Overpayment (Army, Navy, etc.), HUD Loans, GAO Loans (Misc. Types), Mortgage Foreclosures, SBA Loans, Civil Penalties and Coal Mine Penalty and Reclamation Fees.)

I certify that to the best of my knowledge the entries on this Case Designation Sheet are true and correct

Date: September 8, 2017 s/ Joseph N. Kravec, Jr.

ATTORNEY AT LAW

NOTE: ALL SECTIONS OF BOTH FORMS MUST BE COMPLETED BEFORE CASE CAN BE PROCESSED.