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

SEAN NEILAN, individually and on behalf of all others similarly situated,	)	Civil Action No.:
Plaintiff,	)	**CLASS ACTION**
v.	)	**JURY TRIAL DEMANDED**
EQUIFAX INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Sean Neilan ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to him and on information and belief as to all other matters, by and through undersigned counsel, hereby brings this Class Action Complaint against defendant Equifax Inc. ("Equifax" or "Defendant").

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against Equifax for its failure to secure and safeguard the private information of approximately 143 million Americans.

2. On July 29, 2017, Equifax discovered unauthorized access to databases storing the confidential and private consumer information of millions of U.S. consumers.

3. On September 7, 2017, Equifax publicly announced that due to a vulnerability in its systems, its files were accessed by criminals for at least the period of mid-May through July of 2017 ("Security Breach"). The information accessed includes names, social security numbers,

birth dates, addresses, and driver's license numbers, in addition to credit card numbers for some consumers and other documents containing personal identity information ("Private Information").

4. Plaintiff's and Class members' Private Information was accessed and stolen by hackers in the Security Breach.

5. Equifax's security failures enabled and facilitated the criminals' access, obtainment, theft, and misuse of Plaintiff's and Class members' Private Information. Unauthorized persons gained access Equifax's databases through vulnerabilities in its security and executed commands that caused the system to transmit to the unauthorized persons electronic data comprising millions of Americans' Private Information. Equifax's security failures also put Plaintiff and Class members at serious, immediate, and ongoing risk of identity theft, and additionally, will cause costs and expenses to Plaintiff and Class members attributable to responding, identifying, and correcting damages that were reasonably foreseeable as a result of Equifax's willful and negligent conduct.

6. The Security Breach was caused and enabled by Equifax's knowing violation of its obligations to secure consumer information. Equifax failed to comply with security standards and allowed the Private Information of millions collected by Equifax to be compromised by cutting corners on security measures that could have prevented or mitigated the Security Breach.

7. Accordingly, Plaintiff, on behalf of himself and all others similarly situated, asserts claims for violation of the Fair Credit Reporting Act, violation of the Illinois Consumer Fraud Act, violation of Illinois Personal Information Protection Act, and all other substantially similar statutes enacted in other states, and negligence. Plaintiff seeks monetary damages, punitive damages, statutory damages, and injunctive relief, and all other relief as authorized in equity and by law.

II. JURISDICTION AND VENUE

8. The Court has subject matter jurisdiction under 28 U.S.C. § 1331 because Plaintiff's Fair Credit Reporting Act claims arise under the laws of the United States.

9. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

10. The Court has personal jurisdiction over Equifax Inc. because Plaintiff's claims arise out of Equifax's contacts with Illinois.

11. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(2) because a substantial part of the events and omissions giving rise to the claims emanated from activities within this District.

III. PARTIES

12. Sean Neilan resides in Chicago, Illinois, and is a citizen of the State of Illinois. After learning of the Security Breach, Neilan used a tool on Equifax's website to determine whether his Private Information was affected. Using this tool, Neilan determined that his private information was affected by the Security Breach. As a result of the Security Breach, Neilan suffered from the deprivation of the value of his Private Information and will incur future costs and expenditures of time to protect himself from identity theft.

13. Equifax Inc. is a nationwide consumer reporting agency and purveyor of credit monitoring and identity theft protection services. Equifax is a Georgia corporation headquartered in Atlanta, Georgia.

IV. FACTUAL BACKGROUND

14. Equifax is in the business of collecting, assessing, and maintaining the Private Information of approximately 800 million consumers around the world in order to sell this information to third parties in the form of consumer credit reports, consumer insurance reports, or consumer demographic or analytics information. It also sells credit protection and identity theft monitoring services to consumers.

15. In the years preceding Equifax's announcement of the Security Breach, several entities storing large quantities of consumer data caused massive security breaches, including health insurer Anthem, Yahoo, Equifax's competitor, Experian, and many others. Equifax knew or should have known that the Private Information contained in its databases was a prime target for hackers. In fact, it makes many millions of dollars in profits convincing Americans to buy their credit protection and identity theft monitoring services to guard against such breaches and the damages they cause. Despite this, Equifax failed to take adequate steps to secure its systems.

The Equifax Security Breach

16. On September 7, 2017, Equifax announced that its systems were compromised by cybercriminals, reportedly impacting approximately 143 million U.S. consumers. The Security Breach began in mid-May, 2017, and was not detected by Equifax for several months. Equifax admits the Security Breach arose from a "U.S. website application vulnerability" in its systems.

17. Unauthorized persons manipulated Equifax's security vulnerabilities to gain access databases of consumer information. Equifax's systems transmitted to the unauthorized persons during a period of time of over two months without Equifax detecting or limiting the infiltration.

18. After Equifax discovered the Security Breach on July 29, 2017, it waited more than one month before it began notifying impacted consumers on September 7, 2017.

19. In response to the Security Breach, Equifax falsely claims to provide "complimentary identity theft protection and credit monitoring" through the website they created, equifaxsecurity2017.com.

20. In fact, this service is not complimentary and it is not adequate. It is being offered in exchange for waiving significant legal rights, including the Constitutional right to a jury trial, as described in the fine print on the hyperlinked "terms" page, which, among other things, purports to bind users to individual arbitration.[1]

21. The consumer information compromised in the Security Breach includes names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and documents containing personal identity information—all information that is now in the hands of criminals.

Security Breaches Lead to Identity Theft

22. According the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.[2]

23. The Federal Trade Commission ("FTC") cautions that identity theft wreaks havoc on consumers' finances, credit history and reputation and can take time, money, and patience to

[1] *Terms of Use*, available at http://www.equifax.com/terms/ (last visited Sept. 8, 2017).

[2] See *Victims of Identity Theft, 2014*, DOJ, at 1 (2015), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Sept. 8, 2017).

resolve.[3] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[4]

24. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[5] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen private information directly on various Internet websites, making the information publicly available.

25. In fact, "[a] quarter of consumers that received data breach letters [in 2012] wound up becoming a victim of identity fraud."[6]

The Monetary Value of Privacy Protections and Private Information

26. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here

---

[3] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), available at http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited Sept. 8, 2017).

[4] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[5] Companies, in fact, also recognize Private Information as an extremely valuable commodity akin to a form of personal property. *See* John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PERSONAL INFORMATION") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

[6] *One in Four that Receive Data Breach Letters Affected By Identity Theft*, available at http://blog.kaspersky.com/data-breach-letters-affected-by-identity-theft/ (last visited Sept. 8, 2017).

> some time ago that it's something on the order of the life blood, the free flow of information.[7]

27. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[8] Indeed, as a nationwide consumer reporting agency, Equifax's entire line of business depends on the fact that the Private Information of consumers is valuable, both individually and in aggregate.

28. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[9]

29. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit

---

[7] Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited Sept. 8, 2017).

[8] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Sept. 8, 2017).

[9] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited Sept. 8, 2017).

from their Private Information.[10] This business has created a new market for the sale and purchase of this valuable data.[11]

30. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349."[12]

31. The value of Plaintiff's and Class members' Private Information on the black market is substantial. By way of the Security Breach, Equifax has deprived Plaintiff and Class members of the substantial value of their Private Information.

Damages Sustained by Plaintiff and Class Members

32. Plaintiff and other members of the Class have suffered injury and damages, including, but not limited to: (i) an increased risk of identity theft and identity fraud; (ii) improper disclosure of their Private Information, which is now in the hands of criminals; (iii) the value of their time spent mitigating the increased risk of identity theft and identity fraud; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market—for which they are entitled to compensation.

---

[10] Steve Lohr, *You Want My Personal Data? Reward Me for It*, The New York Times, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited Sept. 8, 2017).

[11] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Sept. 8, 2017).

[12] See Department of Justice, *Victims of Identity Theft, 2014*, at 6 (2015), https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Sept. 8, 2017).

33. Plaintiff and the other Class members have suffered additional damages based on the opportunity cost and value of time that Plaintiff and the other Class members have been forced to expend to monitor their financial accounts as a result of the Security Breach.

34. Acknowledging the damage to Plaintiff and Class members, Equifax is instructing consumers to "be vigilant in reviewing their account statements and credit reports," "immediately report any unauthorized activity to their financial institutions" and to "monitor their personal information." Plaintiff and the other Class members now face a greater risk of identity theft.

V. CLASS ACTION ALLEGATIONS

35. Plaintiff brings all counts, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class defined as:

> All persons whose Private Information was affected by the Security Breach that occurred from at least mid-May 2017 through July 2017, including all persons who Equifax's "Check Potential Impact" tool identifies as being affected.

Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

36. In the alternative, Plaintiff brings all counts set forth below on behalf of himself and statewide classes with laws similar to Illinois law, or further in the alternative, an Illinois class (collectively, these alternative classes are referred to as the "Illinois Class") defined as:

> All persons in Illinois (and in those states with laws similar to the applicable law of Illinois) whose Private Information was affected by the Security Breach that occurred from at least mid-May 2017 through July 2017, including all persons who Equifax's "Check Potential Impact" tool identifies as being affected.

Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

37. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

38. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number over one hundred million. The precise number of Class members and their addresses are presently unknown to Plaintiff, but may be ascertained from Equifax's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, or publication.

39. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Equifax failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiff's and Class members' Private Information;

b. Whether Equifax properly implemented its purported security measures to protect Plaintiff's and Class members' Private Information from unauthorized capture, dissemination, and misuse;

c. Whether Equifax took reasonable measures to determine the extent of the Security Breach after it first learned of same;

d. Whether Equifax willfully, recklessly, or negligently failed to maintain and

execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class members' Private Information;

e. Whether Equifax was negligent in failing to properly secure and protect Plaintiff's and Class members' Private Information;

f. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

40. Equifax engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of themselves and other Class members. Similar or identical common law and statutory violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

41. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Equifax's uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Equifax that are unique to Plaintiff.

42. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because his interests do not conflict with the interests of the other Class members he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiff and his counsel.

43. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy,

and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Equifax, so it would be impracticable for Class members to individually seek redress for Equifax's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS

COUNT I
Willful Failure to Comply with the Fair Credit Reporting Act, 15 U.S.C. § 1681n

44. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

45. Equifax is a consumer reporting agency and is subject to the requirements of the federal Fair Credit Reporting Act.

46. Plaintiff's and Class members' Private Information are consumer reports under FCRA, because the information bears on, among other things, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical/medical conditions, and mode of living, and is used or collected, in whole or in part, for the purpose of establishing Plaintiff's and the other Class members' eligibility for credit or insurance to be used primarily for personal, family, or household purposes.

47. FCRA enumerates the exclusive purposes for which a consumer reporting agency can furnish consumer reports. 15 U.S.C. § 1681b. FCRA also requires that:

> Every consumer reporting agency shall maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title. These procedures shall require that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose.

15 U.S.C. § 1681e.

48. Defendant willfully, knowingly, or with reckless disregard, failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b when it enabled and facilitated the Security Breach. Defendant failed to adequately vet users of its consumer reports, failed to inquire into suspicious circumstances despite possessing knowledge that put it on inquiry notice, and failed to reasonably monitor its customers' acquisition and use of consumer reports.

49. Defendant willfully, knowingly, or with reckless disregard, failed to comply with the FCRA's requirements with respect to Plaintiff and the other Class members. As a result of Defendant's failures, Defendant transmitted Plaintiff's and other Class members' Private Information to criminals for illegitimate and unauthorized purposes.

50. As a further direct and foreseeable result of Defendant's willful noncompliance with FCRA, Plaintiff's and the other Class members' Private Information will remain posted online in the public domain, compromised, and in possession of unauthorized third parties with fraudulent intent.

51. Plaintiff and the other Class members seek any actual damages they have sustained, or in the alternative not less than $100 and not more than $1,000 in statutory damages; punitive

damages as the court may allow, the costs of this action together with reasonable attorney's fees as determined by the court.

COUNT II
Negligent Failure to Comply with Fair Credit Reporting Act, 15 U.S.C. § 1681o

52. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

53. Defendant negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b when it enabled and facilitated the Security Breach. Defendant failed to adequately vet users of its consumer reports, failed to inquire into suspicious circumstances despite possessing knowledge that put it on inquiry notice, and failed to reasonably monitor its customers' acquisition and use of consumer reports.

54. Plaintiff's and the other Class members' Private Information was wrongfully furnished to criminals as a direct and foreseeable result of Defendant's negligent failure to adopt and maintain such reasonable procedures.

55. As a direct and foreseeable result, Plaintiff's and the other Class members' consumer reports were accessed, made accessible to, stolen, furnished, and sold to unauthorized third parties for illegitimate and unauthorized purposes.

56. As a result of Defendant's negligent violations of FCRA, as described above, Plaintiff and the other Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail above.

57. Plaintiff and the other Class members, therefore, are entitled to compensation for their actual damages, as well as attorneys' fees, litigation expenses, and costs, pursuant to 15 U.S.C. § 1681o(a).

COUNT III
Violation of Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/2
Unfair Business Practices

58. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

59. Plaintiff and the other members of the Class were subjected to Defendant's unfair or deceptive acts or practices, in violation of 815 Ill. Comp. Stat. 505/2, in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

60. Defendant willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

61. Defendant benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

62. Defendant's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonable avoidable by consumers.

63. Defendant's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

64. Plaintiff and the other members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money

incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

65. Plaintiff's and the other Class members' injuries were proximately caused by Defendant's violations of the ICFA, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT IV
Violation of Illinois Consumer Fraud Act, 815 ILCS 505/2
Deceptive and Unfair Business Practices

66. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

67. Defendant falsely represents to Plaintiff and the other Class members, and all others that Defendant offers complimentary one-year enrollment of its Trusted ID Premier product for affected persons.

68. In actuality, Defendant purports to bind persons who enroll in the service to a set of terms, posted on its website, which include a binding arbitration provision. As a result, Defendant's offer is not complimentary and employs deception and coercion in an unconscionable effort to bind affected persons to arbitrate their claims.

69. Plaintiff and the other Class members seek an injunction against Defendant from making misrepresentations during the course of attempting to comply with its legal obligations to notify affected individuals.

70. Plaintiff and the other Class members seek a declaration that any availment of Defendant's purportedly complimentary credit protection services do not waive claims against Defendant or otherwise bind or constitute consent or agreement in any way.

COUNT V
Violation of Illinois Personal Information Protection Act
Failure to Provide Expedient Notice, 815 ILCS 530/10

71. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

72. Plaintiff and the Class members' Private Information is Personal Information within the meaning of 815 ILCS 530/5.

73. Defendant is a Data Collector within the meaning of 815 ILCS 530/5.

74. Defendant violated 815 ILCS 530/10(a) by failing to notify Illinois residents at no charge of the Security Breach in the most expedient time possible and without unreasonable delay. Defendant learned of the Security Breach as early as July 2017 but failed to notify affected persons until September 7, 2017.

75. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach and violation of PIPA, including the increased risk of identity theft that resulted and continues to face them.

76. Plaintiff's and the other Class members' injuries were proximately caused by Defendant's violations of the PIPA, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT VI
Violation of Illinois Personal Information Protection Act,
Failure to Implement and Maintain Reasonable Security, 815 ILCS 530/45

77. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

78. Plaintiff and the Class members' Private Information is Personal Information within the meaning of 815 ILCS 530/5.

79. Defendant is a Data Collector within the meaning of 815 ILCS 530/5.

80. Defendant violated 815 ILCS 530/45 by failing to implement and maintain reasonable security measures to protect the Private Information from unauthorized access, acquisition, destruction, use, modification, or disclosure.

81. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach and violation of PIPA, including the increased risk of identity theft that resulted and continues to face them.

82. Plaintiff's and the other Class members' injuries were proximately caused by Defendant's violations of the PIPA, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT VII
Negligence

83. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

84. Equifax owed numerous duties to Plaintiff and the other members of the Class. These duties include the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect Private Information in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and the other members of the Class of the Security Breach.

85. Equifax knew or should have known the risks of collecting and storing Private Information and the importance of maintaining secure systems. Equifax knew of the many breaches that targeted other entities in the years preceding the Security Breach.

86. Equifax knew or should have known that its systems did not adequately safeguard Plaintiff's and the other Class members' Private Information.

87. Equifax breached the duties it owed to Plaintiff and Class members in several ways, including:

d. by failing to implement adequate security systems, protocols and practices sufficient to protect customer Private Information and thereby creating a foreseeable risk of harm;

e. by failing to comply with the minimum industry data security standards; and

f. by failing to timely and accurately discovery and disclose to customers that their Private Information had been improperly acquired or accessed.

88. But for Equifax's wrongful and negligent breach of the duties it owed to Plaintiff and the other Class members, their Private Information would not have been compromised.

89. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Equifax's negligent conduct.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this complaint so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Equifax, as follows:

A. Certifying the Class as requested herein, designating Plaintiff Sean Neilan as Class Representative, and appointing Ben Barnow of Barnow and Associates, P.C. as Class Counsel;

B. Ordering Equifax to pay actual damages to Plaintiff and the other members of the Class;

C. Entering an injunction against Equifax, prohibiting the deceptive conduct described in Count IV;

D. Ordering Equifax to pay statutory damages to Plaintiff and the other members of the Class;

E. Ordering Equifax to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

F. Ordering Equifax to pay attorneys' fees and litigation costs to Plaintiff;

G. Ordering Equifax to pay both pre- and post-judgment interest on any amounts awarded as allowable by law; and

H. Ordering such other and further relief as may be just and proper.

Date: September 8, 2017

Respectfully submitted,

Sean Neilan, individually and on behalf of all others similarly situated,

/s/ Ben Barnow

Ben Barnow
Erich P. Schork
Anthony L. Parkhill
Jeffrey D. Blake
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602

Tel: (312) 621-2000
Fax: (312) 641-5504
b.barnow@barnowlaw.com
e.schork@barnowlaw.com
aparkhill@barnowlaw.com
j.blake@barnowlaw.com

Timothy G. Blood
BLOOD HURST & O'REARDON, LLP
701 B Street, Suite 1700
San Diego, CA 92101
Tel: (619) 338-1100
Fax: (619) 338-1101
tblood@bholaw.com

Richard L. Coffman
THE COFFMAN LAW FIRM
First City Building
505 Orleans Street, Suite 505
Beaumont, TX 77701
Tel: (409) 833-7700
Fax: (866) 835-8250
rcoffman@coffmanlawfirm.com