

**UNITED STATES DISTRICT COURT  
DISTRICT OF CONNECTICUT**

NATALIE QUAGLIANI, Individually and  
on behalf of others similarly situated,

Plaintiffs,

v.

EQUIFAX, INC., EQUIFAX HEALTH  
SERVICES and EQUIFAX CREDIT  
INFORMATION SERVICES, INC.,

Defendants.

.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....

Civ. Action No. \_\_\_\_

JURY TRIAL DEMANDED

**CLASS ACTION COMPLAINT**

Plaintiff Natalie Quagliani ("Plaintiff" or "Quagliani"), individually and on behalf of all other Connecticut residents similarly situated, as and for her class action complaint against Defendants Equifax Inc. (also doing business as Equifax Health Services), and Equifax Credit Information Services, Inc. (sometimes hereinafter collectively "Defendants" or "Equifax"), alleges as follows:

**NATURE OF THE CASE**

1. Equifax is one of the largest U.S. credit rating agencies. By its willful and negligent actions, Equifax enabled a series of data breaches of monumental proportions starting no later than May 2017 and continuing until late July 2017. As a result, criminal hackers were reportedly able to misappropriate the most sensitive personal financial information of nearly 145 million persons in the United States. This personal information includes, without limitation, full social security numbers, credit card numbers, loan information, drivers' license numbers, mortgage data, birth dates, address histories, parental names, and other personal information highly useful to people engaged in identity theft.

2. Equifax admits being aware of security holes in its cyber defense as early as March 2017. Equifax admits that it was specifically warned in March 2017 by the U.S.

Department of Homeland Security of a certain gap in its online security, yet Equifax decided to do nothing to close the vulnerability notwithstanding there was a known, readily available fix/patch that it could easily access.

3. No later than the end of July 2017 and, upon information and belief, much earlier than July, Equifax discovered a massive intrusion and theft of data by criminal hackers. Despite the fact that Equifax knew or should have known that the data breach had compromised the personal financial information of more than 100 million U.S. consumers, Equifax took no action to notify the public of the massive data breach until approximately September 7, 2017, further compounding the injury.

4. The Plaintiff brings this class action, both individually and on behalf of a class of similarly situated Connecticut residents, against the Defendants to recover statutory damages for multiple violations of the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 (the "FCRA") pursuant to 15 U.S.C. §§ 1681n and 1681o. The Plaintiff and Class Members further seek relief under certain Connecticut laws and statutes including as follows: (i) an Act on the Protection of Social Security Numbers and Personal Information, C.G.S. § 42-470 *et seq.*; (ii) Section 36a-701b of the Connecticut General Statutes, which requires that persons holding such sensitive personal financial data of Connecticut consumers must notify any affected consumers of a data breach within a reasonable period of time under the circumstances; (iii) Section 38a-999b of the Connecticut General Statutes, which requires healthcare utilization review companies such as Equifax Health Services to provide the public with data breach notification in the same manner as under Section 36a-701b; (iv) and the Connecticut Unfair Trade Practices Act ("CUTPA"), C.G.S. § 42-110(b) and 42-110g.; and (vi) for common law negligence.

5. This is a consumer class action lawsuit brought by Plaintiff, individually and on behalf of all others similarly situated residents of the State of Connecticut (*i.e.*, sometimes hereinafter referred to as the "Class" or "Class Members"), who have had their above described personal information held by Equifax -- including their names, social security numbers, birth dates, addresses, drivers' license numbers, credit card numbers and other personal identifying information (hereinafter sometimes referred to collectively for ease of reference as "Individual Identification Information" or "3I") -- unlawfully disclosed to unnamed third parties (hereinafter sometimes referred to as the "Data Breach") due to Equifax's intentionally careless and negligent handling of such information and outrageous failure to properly secure Plaintiff's 3I and that of the other Class Members after Equifax was specifically warned by the U.S. government of a clear and present danger that such 3I could and likely would be stolen by hackers. Excluded from the class are all attorneys for the class, officers and members of any entity with an ownership interest in Equifax, any judge who sits on the case, and all jurors and alternate jurors who in the end sit on the case.

6. The Plaintiff alleges facts regarding herself based on personal knowledge, and upon information and belief as to all other allegations, provided however, that the Plaintiff reasonably believes that substantial evidentiary support will exist for any allegations made upon information and belief after a reasonable opportunity for discovery.

7. Equifax is a global provider of information solutions and human resource business process outsourcing services for consumers, businesses, and governments and is best known for acting as a credit rating agency. Equifax is among the largest credit reporting agencies in the United States, possessing 3I on over 800 million individuals and 88 million businesses worldwide.

8. Through its division Equifax Healthcare Services, Equifax also provides healthcare "utilization review services" to, *inter alia*, Connecticut hospitals and physician providers, and to Connecticut state Medicaid agencies, as defined in section 38a-591a of the Connecticut General Statutes, which includes Equifax Healthcare Services using formal techniques to monitor the appropriateness of health care services in health care settings, including evaluating requirements to obtain a clinical evaluation by a health care professional other than the one originally making the recommendation for a proposed health care service, and certification of health care services.

9. By virtue of acting as a credit rating agency and as a provider of healthcare utilization review services, Equifax had a statutory duty to notify affected persons of the Data Breach within a reasonable time pursuant to C.G.S. §§ 36a-701b and 38a-399b, but intentionally failed to do so after it was warned by the U.S. government about the potential of irreparable harm that could result.

10. Equifax owed a legal (as well as moral and ethical) duty to consumers, such as Quagliani and the Class Members, to use reasonable care, in possessing and using their 3I, which included a duty to protect their personal information and credit information from unauthorized access by third parties and criminal hackers. Equifax failed in this legal and moral duty, knowing full well that any such failure on Equifax's part posed extreme risks of widespread identity theft, credit fraud, and invasion of privacy, into perpetuity, for any persons (including Quagliani and the Class Members) whose 3I might be misappropriated from Equifax by criminal hackers.

11. Equifax disregarded the Plaintiff's and Class Members' privacy and informational security rights when it had the knowledge, information and belief that a Data

Breach was possible if not likely and, intentionally, willfully, recklessly or negligently failed to take the necessary precautions required to safeguard and protect their 3I from unauthorized disclosure and misuse, and by failing to implement appropriate cyber-security protocols, policies, and procedures. As a direct and proximate result of Equifax's failures, the Plaintiff's and Class Members' 3I held by Equifax was predictably compromised and stolen.

12. Having been specifically warned by the U.S. Department of Homeland Security, Equifax admittedly knew at least as early as March 2017 that Apache Struts, an open-source software framework that Equifax used to build its websites had a specific vulnerability that exposed Equifax to a serious risk of a possible data breach. Equifax also knew that a patch was being offered by Apache Struts to fix at least one of the known vulnerabilities. Nonetheless, showing callous disregard for the security of its consumers' 3I and obviously necessarily aware of the cataclysmic nature of the injury that could result to hundreds of millions of people in the event of a large scale data breach, Equifax still failed to take necessary corrective action and simply ignored the known vulnerabilities of Apache Struts so as to leave much of all of its customers' 3I in grave danger of theft.

13. Further compounding the catastrophic injury caused by the Data Breach and evidencing Equifax awareness of its own wrongdoing, Equifax further violated the rights of the Plaintiff and the other Class Members by purposefully not notifying them within a reasonable period of time after Equifax learned of the Data Breach. Indeed, upon information and belief, Equifax was aware that it had suffered a major hacking attack in mid-May 2017, and then again in July 2017, but did not report the Data Breach to the public until September 7, 2017.

14. It is deeply troubling that apparently Equifax was seemingly motivated to drag its heels notifying consumers, not only to avoid the embarrassment and mortification that would

inevitably flow from disclosing Equifax's gross neglect of duty and nearly irreparable injury caused by the exposure of almost half of U.S. consumers' 3I, but also to allow additional time for certain senior executives of Equifax to dump their own Equifax stock holdings through illegal insider trading.

15. By failing to disclose the earliest discovered breach to its consumers, and failing to take any and all measures to prevent future data breaches of a similar nature, Equifax left open the possibility of a larger breach, which Equifax admitted occurred from mid-May 2017 through the end of July 2017, culminating in hackers exploiting a vulnerability in the Equifax website software to gain access to 3I on as many as 146 million U.S. consumers.

16. Furthermore, it has been reported that after the massive data breach was finally reported by Equifax to consumers at the end of the first week of September 2017, Equifax compounded the problem by directing victims to a fake phishing site further compromising their 3I information. *See* Tribute Media Wire, *Equifax Has Been Sending Concerned Customers to a Fake Phishing Site*, KTLA5 (Sept. 20, 2017), <http://ktla.com/2017/09/20/equifax-has-been-sending-concerned-customers-to-fake-phishing-site/>.

17. Upon information and belief, Equifax's failure to notify the public of the above referenced data breaches within a reasonable time after detection of same by Equifax, was intentional, wanton and showed a callous disregard on Equifax's part for the need to protect the 3I of hundreds of millions of persons that Equifax had taken upon itself to safeguard.

18. Equifax owed a legal duty to protect the general public (including the Class) from clearly foreseeable massive harm should their 3I fall into the wrong hands.

19. Despite the ultra-hazardous nature of Equifax acting as custodian of hundreds of millions of persons' most sensitive 3I, Equifax failed to implement even the most basic security

procedures to safeguard the 3I. Equifax also failed to take all immediate necessary steps to prevent additional intrusions by cyber criminals after Equifax was specifically notified that there was a readily patchable hole in its cyber security.

20. Compounding the harm, after learning of the Data Breach Equifax purposefully failed to notify the public of the massive loss of 3I to criminal hackers resulting from Equifax's gross negligence within a reasonable period of time. Equifax's concealment of the Data Breach constitutes an unfair trade and deceptive trade practice.

21. The Data Breach has had a devastating effect on Quagliani and the Class Members, causing them to suffer injury of a permanent (as in forever) increased risk of identity theft, invasion of privacy and economic losses, including monetary loss in the form of incurring future costs for the remainder of the Class Members' natural lifetimes entailed in the taking of preventive or ameliorative measures (including, without limitation, the need to purchase credit monitoring and credit repair services forever) to try to at least partially mitigate the potential for inevitable large scale criminal misuse of the 3I by various criminal elements around the globe.

22. A leading provider of research on identity theft, Jevilin Strategy & Research, in its 2013 Identity Fraud Report ("the Javelin Report") has opined that as a general rule of thumb at least one out of every four individuals whose 3I is compromised by a reported security breach, will suffer some type of future identity fraud or identity theft. *See* Al Pascual, *2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters* Javelin (Feb. 20, 2013) <https://www.javelinstrategy.com/coverage-area/2013-identity-fraud-report-data-breaches-becoming-treasure-trove-fraudsters>. In the present case, upon information and belief, the risk would seemingly be even more enhanced given the breadth of the 3I stolen in this case, which constituted, upon information and belief, individual consumers' complete centralized credit files,

as distinguished from some prior data breaches involving retailers and other merchants (who may have only had partial 3I about consumers being accessed but not their complete credit file with the level of detail possessed by a credit ratings agency like Equifax).

23. Among a few limited examples of the malicious mayhem that the cyber criminals can potentially use the 3I that they extracted from Equifax include, to name just a few: (a) the filing of a tax refund in one's name and stealing the refund; (b) draining bank and securities accounts; (c) open new financial accounts, (d) conducting unauthorized financial research into individuals' financial accounts to invade their privacy; (e) running up charges on credit cards; (f) getting medical treatment on another's health insurance; and (g) opening new utility accounts, to name just a few.

24. Unfortunately, it is quite difficult for Class Members whose 3I has been stolen as a result of Equifax's gross negligence to obtain a new, replacement Social Security number, as one must actually show the existing number is actually being used fraudulently, and that the consumer has done everything possible to fix the problems associated with use. Even if a new social security number is obtained, the person obtaining it will very likely still encounter other problems, complications, and confusion due to the fact that others (some legitimately and some criminally) still have their old social security number.

25. Upon information and belief, 3I is very valuable on the cyber black market. Thus, it is seemingly likely that a black market will develop for trading in the 3I that has been stolen and is now largely irretrievably due to Equifax's negligence, with various cyber criminals no doubt purchasing or otherwise acquiring the 3I to facilitate their various nefarious and illegal uses and purposes. Again, there is no total fix. Indeed, Equifax has created a problem that will exist into perpetuity, *inter alia*, as there is no practical way to retrieve the 3I once it is widely



disseminated on the web to various criminal elements around the globe.

26. At all times herein relevant, Equifax was aware, and reasonably should have been aware, of the highly sensitive nature of the information they held on behalf of consumers, and the significant harm that would be caused to consumers should the same be susceptible to theft by international criminal syndicates. By Equifax's woeful failure to prevent the previously described data breaches, Equifax has caused the Plaintiff and the Class Members to be harmed, again potentially permanently, *inter alia*, due to out-of-pocket costs for future credit monitoring services and third-party credit repair, which even under the best of circumstances is limited in its ability to make the Plaintiff and Class Members whole again.

27. Thus, due to Equifax's wrongful actions and inactions, Quagliani and the Class Members have been placed at an imminent, as well as continuing, risk of suffering both present and future identity theft and fraud. The clear and present danger posed by this threat will require Quagliani and other class members to devote considerable time and effort to mitigate the resulting inevitable harm. At the bare minimum, it will seemingly require the entire Class to purchase a lifetime of future credit monitoring, as well as credit repair services as their respective 3I is misused in the future. As such, Quagliani and the Class Members have suffered, and will continue to suffer for the remainder of their natural lives, economic damage and other harm to which they are entitled compensation, in amounts to be proven at trial.

#### **JURISDICTION AND VENUE**

28. Federal subject matter jurisdiction for the First and Second Causes of Action exists pursuant to the FCRA, 15 U.S.C. §§ 1681 *et seq.* and 28 U.S.C. §§ 1331.

29. The Court also has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §1332(d), *inter alia*, because the aggregate amount

in controversy exceeds \$5 million dollars and there is diversity between a plaintiff and a defendant.

30. This Court has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C § 1367.

31. This Court has personal jurisdiction over Equifax because Equifax at all relevant times conducts, and continues to conduct, business in Connecticut and personal jurisdiction further exists pursuant to Connecticut's long arm statute. C.G.S. §§ 33-929(f).

32. Venue is proper pursuant to 28 U.S.C. § 1391(b)(1)-(2) and (c).

#### **PARTIES**

33. Plaintiff Natalie Quagliani is a natural person residing in West Haven, Connecticut. Upon information and belief, Quagliani's 3I was in the custody of Equifax as of March 2017 through the present time. According to certain verification systems created and provided by Equifax to consumers so that they can attempt to determine if each of their respective 3I was compromised by the Data Breach, Quagliani was told that she was a probable victim of the Data Breach. Quagliani is a “consumer” within the meaning of 15 U.S.C. § 1681a(c).

34. Defendant Equifax Inc. ("Equifax") is a Delaware corporation with principal executive offices located at 1550 Peachtree Street, NE, Atlanta, Georgia 30309. Equifax is authorized to, and does conduct, business in the State of Connecticut. Equifax is a “consumer reporting agency” within the meaning of 15 U.S.C. § 1681a(f). Equifax is regularly engaged in the business of evaluating and dispersing, and assembling, information concerning consumers for the purpose of furnishing to third parties “consumer reports” within the meaning of 15 U.S.C. § 1681(a)(d). As such, Equifax Inc.’s conduct is governed by, and Equifax is subject to, *inter alia*, the remedies provided by the FCRA.

35. Equifax Healthcare Services ("Equifax Healthcare") is, upon information and belief, a division of Equifax, with its principal executive offices also located at 1550 Peachtree Street, NE, Atlanta, Georgia 30309. Equifax d/b/a Equifax Healthcare Services is a utilization review "company" within the meaning of C.G.S. §§ 38a-999b and 38a-591a.

36. Defendant Equifax Credit Information Services, Inc. ("Equifax Credit") is a Georgia corporation with its principal place of business located at 1550 Peachtree Street, NW, Atlanta, Georgia 30309. Equifax Credit is authorized to, and does conduct, business in the State of Connecticut.

#### **CLASS ALLEGATIONS**

37. Plaintiffs file this complaint as a Connecticut class action lawsuit. The Connecticut Class consists of Connecticut resident consumers who:

- Had 3I either stored, possessed or collected, by Equifax in 2017; and
- Who are now subject to the risk of data loss and credit harm, as well as identity theft, and invasion of privacy, or who paid for a third-party credit monitoring service, or security freeze at one or more credit facility, due to Equifax's negligent handling of their 3I in connection with the Data Breaches, and/or its negligent handling of informing the public of the data breach in a reasonable period of time; and
- Have been identified by Equifax as persons whose 3I have been presumptively comprised by the Data Breach; and
- Who are neither attorneys for the class, officers and members of Equifax, including officers and members of any entity with an ownership interest in Equifax, and any judge who sits on the case, and all jurors and alternate jurors who sit on the case; and
- Who has suffered injuries as alleged in this complaint directly or proximately caused by Equifax's negligent failure to adequately protect the 3I database from unauthorized access by third-party hackers.

38. Joinder is impractical in this case given the numerosity of the class.

39. Common questions of fact and law predominate over questions affecting

individual class members.

40. Common questions include, *inter alia*, whether Quagliani and the Class members are entitled to equitable relief, whether Equifax acted negligently, whether Equifax is liable for the Data Breach under the FRCA, C.G.S. § 42-470 *et seq.*, CUTPA (C.G.S. § 42-110g) and based on common law negligence, whether Equifax failed to provide the public with timely notification after learning of the Data Breach in violation of C.G.S. §§ 36a-701b, 38a-999b, and whether Quagliani and the Class are entitled to recovery money damages.

41. Quagliani's claims are typical of the claims of the Class Members, *inter alia*, because each suffered a risk of loss and credit harm and identity theft by Equifax's negligent failure to safeguard their data, the injuries suffered by Quagliani and the Class Members are largely identical in nature and effect, and their claims for relief are based on the same legal theories.

42. Quagliani will fairly and adequately protect and represent the interest of the Class Members because her injuries are the same and her claims are typical of the claims of the Class members.

43. This class action is superior to other methods for the fair and efficient adjudication of the case because common questions of law and fact predominate over other factors affecting only individual members, individual class members have little interest in controlling the litigation primarily because of the high cost of such action and the relatively small amounts of damages per class member, and because Quagliani and her attorneys will vigorously pursue the claims.

44. The availability through discovery of Equifax's business records reflecting which specific Connecticut consumers had their 3I stolen by virtue of the Data Breach will facilitate

proving the ascertainability of the Class, proof of Class claims, processing Class claims, and distributions of any recoveries to the Class.

### **FACTS COMMON TO ALL COUNTS**

45. Equifax was founded in 1899, and is headquartered in Atlanta, Georgia.

46. Equifax is a global provider of information solutions, and is one of three nationwide credit-reporting companies that tracks and rates the financial history of consumers in the U.S.

47. Upon information and belief, at the time of the Data Breach, Equifax had custody of 3I on over 800 million individuals and 88 million businesses worldwide.

48. At all times herein relevant, Equifax has stated, represented, and otherwise assured the public that Equifax utilizes robust data protection protocols to safeguard the 3I in its custody.

49. Upon information and belief, Equifax's affiliate, Equifax Healthcare Services, aids hospital and physician providers and state Medicaid programs in the admission, discharge and transmit process, optimizing resources and improving patient contact, and in utilization review.

50. In a report dated September 7, 2017, Equifax asserted that a mid-May 2017 breach was discovered on July 29, 2017 where perpetrators gained access to at least one of its servers, and retrieved certain files, by exploiting “a ... website application vulnerability.”

51. Later Equifax admitted that a similar data breach had also occurred in March 2017. See *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*,

EQUIFAX (Sept. 15, 2017) <https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832>.

52. Upon information and belief, Equifax recognized the existence and seriousness of the March 2017 and May 2017 data breaches well before July 29, 2017.

53. Thus, Equifax took months to notify consumers of the two data breaches thus knowingly and willfully leaving potentially hundreds of millions of persons in the U.S. and around the world exposed to identity theft without any fair warning and with little chance to protect themselves.

54. During the period of Equifax silence on the Data Breaches, at least three Equifax executives who were aware of the occurrence of the Data Breaches, and upon information and belief many more than that, sold Equifax stock holdings worth approximately \$1.8 million dollars.

55. In its September 7, 2017 press release Equifax asserted that the unauthorized access occurred “from mid-May through July 2017,” without notifying the public and that Equifax had been aware of the specific vulnerability since March 2017 and took no action to prevent the Data Breach.

56. Equifax further noted in the above referenced press release that among the 31 accessed, credit card numbers for approximately 209,000 U.S. consumers and certain dispute documents for 182,000 U.S. consumers were accessed, as well as certain “limited personal information” for certain UK and Canadian residents.

57. Upon information and belief, Equifax falsely asserted in the same press release that it discovered the unauthorized access on July 29, 2017.

58. As a result of the Data Breach, Quagliani and Class Members are, upon

information and belief, now subject to a greatly enhanced, permanent risk (indeed, probability) of future identity theft and criminal misuse of their most sensitive personal financial data.

59. Upon information and belief, Equifax failed to adequately safeguard the 3I that it possessed despite knowing that the 3I was subject to strict privacy and security protections of Federal Fair Credit Reporting Act (the "FCRA"), which requires Equifax to adopt and enforce reasonable procedures to keep sensitive information confidential. Equifax also violated 15 U.S.C. § 1681(b) and C.G.S. §§ 42-470 *et seq.* requiring Equifax to affirmatively protect the Social Security numbers of Connecticut residents, which Equifax failed to do when it knew of a possible and likely threat and failed to act, leaving its customer's 3I vulnerable.

60. Upon information and belief, and in an attempt to increase its profits and/or also due to general lack of care about the welfare of the consumers for which Equifax is entrusted with their 3I, Equifax negligently (and willfully) failed to maintain adequate safeguards to protect the 3I of Quagliani and the Class Members from unauthorized access by hackers, and failed to devote sufficient financial resources and attention to combatting risks posed to the data with which Equifax was entrusted despite obviously being aware of the foreseeable horrific and almost irreparable damage that would inevitably flow from any large scale data breach.

61. Due to Equifax's failure to implement basic adequate security procedures, it now appears that the 3I of more than 145 million Americans is now in the hands of third parties including criminal hackers.

62. In contravention of, *inter alia*, C.G.S. §§ 36a-701b, 38a-999b and 42-110b, Equifax purposefully delayed and otherwise failed to properly and timely notify Quagliani and the Class members, or any Connecticut government authorities, regarding this stolen protected 3I information, depriving the Class Members of any ability they would have otherwise had to at

least start to take some immediate efforts to attempt to reduce their risk of identity theft and criminal misuse of their 3I flowing from the Data Breach.

63. Due to Equifax's above referenced negligence, recklessness and callous disregard for the welfare of the hundreds of millions of people whose most sensitive personal financial data has now seemingly been permanently compromised, all in violation of applicable Federal and Connecticut state law, Quagliani and Class members face a substantially increased immediate and future risk of identity theft into perpetuity.

64. More specifically, Quagliani and the Class have suffered significant economic damage in that they will almost certainly be required to incur significant costs for the rest of their respective lives, in undertaking mitigating and/or ameliorative measures, such as purchasing credit monitory services or credit repair services from third party providers, as well as the institution of credit security freezes, an invasion of their privacy rights in their 3I, and deprivation of rights they possess under the FCRA.

65. Furthermore, Quagliani and Class Members have a continuing interest in ensuring that their 3I that remains in the possession of Equifax is protected and safeguarded.

66. Upon information and belief, no law enforcement agency determined that earlier notification to affected Connecticut residents would have impeded any ongoing criminal investigation. Nor does it appear that any law enforcement agency requested Equifax to delay the statutorily required notification of the Data Breach to consumers in the present instance.

67. Upon information and belief, Equifax failed to effectively supervise and train its workforce (including both employees and independent contractors) on the policies and procedures with respect to the appropriate maintenance, use, and disclosure of protected 3I, as is evidenced by, *inter alia*, the errors committed after the notification of the breach in which



employee provided information related to spoof sites for aid in correcting damage from the breach.

**FIRST CLAIM FOR RELIEF (WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT, 15 U.S.C. §§ 1681)**

68. Plaintiffs incorporate by reference all preceding paragraphs numbered 1 to 67 of this Complaint as if fully set forth herein.

69. A fundamental purpose of the FCRA is to protect consumer privacy rights. 15 U.S.C. § 1681(a).

70. Protection of consumer privacy under the FCRA includes the adoption of reasonable procedures to keep 3I information confidential. 15 U.S.C. § 1681(b).

71. Equifax regularly assembles consumer information contemplated by the FCRA and utilized interstate commerce to furnish such information in the form of various types of consumer reports to third parties.

72. Quagliani and the Class Members are consumers within the meaning of 15 U.S.C. §1681a(f).

73. Quagliani's and the Class Members' 3I constitute "Consumer Reports" under the FCRA within the meaning of 15 U.S.C. §1681a(d)(1), *inter alia*, because this information bears on each member of the Class's credit worthiness, credit capacity, character, reputation, credit standing, and mode of living, and is used or collected, in whole or in part, for the purpose of furnishing such information to third parties. 15 U.S.C. § 1681a(f).

74. Equifax is a consumer reporting agency within the meaning of 15 U.S.C. § 1681a(f).

75. 15 U.S.C. §1681(b) of the FCRA requires the adoption of reasonable procedures with regard to the confidentiality and proper utilization of personal and insurance information.

76. Equifax was knowledgeable of its legal obligations regarding data security and data breaches under the FCRA as these obligations are set forth in the plain language of the FCRA, as well as 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(2)(E).

77. 15 U.S.C. §1681(b) of the FCRA requires “that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information . . . .”

78. Upon information and belief, Equifax failed to adopt and maintain these and other reasonable procedures designed to limit the furnishing of consumer reports listed under 15 U.S.C. § 1681(b).

79. Indeed, upon information and belief, Equifax failed to take reasonable and appropriate measures to protect 3I of consumers whose information Equifax routinely collects, stores and sells to third parties in the ordinary course of Equifax's business.

80. Further, Equifax failed to notify Quagliani and the Class Members of the Data Breach in a reasonable period of time as required under the FCRA.

81. Upon information and belief, Equifax’s violation of the FCRA was willful, or at the very least reckless. Due to Equifax’s willful or reckless failure to adopt and maintain reasonable procedures to limit its 3I data to those purposes listed under 15 U.S.C. §§ 1681(b), the 3I belonging to Quagliani and the Class Members was compromised, stolen, and disseminated to third parties, causing harm to Quagliani and the Class Members.

82. Due to the direct and proximate results of Equifax's willful or reckless violations of the FRCA, Quagliani and class members are each entitled to recover their actual damages of not less than \$100 per violation up to a maximum of \$1,000 each per violation, with Quagliani and all of the Class Members, upon information and belief, all incurring actual damages well in excess of \$1,000 each, plus an award of punitive damages given the willful nature of Equifax's breaches of the FCRA, plus Plaintiff's reasonable attorneys' fees and costs should they prevail in this action, all pursuant to 15 U.S.C. § 1681n(a)(3).

**SECOND CLAIM FOR RELIEF: NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT, 15 U.S.C. §§ 1681o.**

83. The Plaintiff and Class Members incorporate by reference all preceding paragraphs numbered 1 to 82 as if fully set forth herein and further alleges as follows:

84. A fundamental purpose of the FCRA is to protect consumer privacy rights. 15 U.S.C. § 1681(a).

85. Upon information and belief, Equifax negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports for the purposes listed under 15 U.S.C. § 1681(b).

86. Due to Equifax' negligence the 3I belonging to Quagliani and the Class Members were wrongfully disseminated to the public through a data breach and the resulting injury to Quagliani and the Class Members was a direct and foreseeable result of Defendant's failure to adopt and maintain such reasonable procedures.

87. As a direct and proximate result of Equifax's negligent violations of FCRA, the 3I of Quagliani and the Class Members were made accessible to unauthorized third parties in the public domain, and was subsequently compromised and stolen.

88. As a direct and proximate result of Equifax's negligent violations of the FCRA,

Quagliani and the Class Members were, and continue to be, injured and suffer damages described above.

89. Therefore, Quagliani and the Class Members are entitled to compensation for their actual damages in an amount to be proven at trial, as well as their reasonable attorneys' fees, litigation expenses, and costs pursuant to 15 U.S.C. §1681o(a)(1)-(2).

**THIRD CLAIM FOR RELIEF: VIOLATION OF C.G.S. § 42-470 ET SEQ. – PROTECTION OF SOCIAL SECURITY NUMBERS**

90. The Plaintiff and Class Members incorporate by reference all preceding paragraphs numbered 1 to 89 as if fully set forth herein and further alleges as follows:

91. C.G.S. § 42-470 requires that any individual transmitting an individual's social security number over the internet, must assure that the connection is secure and the social security number is encrypted. It further prohibits any person from intentionally publishing, or otherwise making available social security numbers to the general public.

92. C.G.S. § 42-471 requires that "any person in possession of personal information of another person shall safeguard the data, computer files, and documents containing the information from misuse by third parties, and shall destroy, erase or make unreadable such data, computer files and documents prior to disposal" of same. "Personal information" for purposes of this section is defined "as information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number, [but] does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media."

93. Equifax failed to safeguard the personal information of the Plaintiff and Class

Members as is statutorily required, causing the Data Breach.

94. C.G.S. §§ 42-471 and C.G.S. §§ 42-472(a) contemplate that individual Connecticut consumers can bring an action to recover their damages for said violations.

95. C.G.S. §§ 42-470 and C.G.S. §§ 42-471 provide for civil penalties that are deposited into a privacy protection guaranty and enforcement account, and C.G.S. § 42-472a(c) provides after any individual obtains a final non-appealable judgment in his or her favor for violation of any provisions of C.G.S. §§ 42-470 through C.G.S. §§ 42-472(b) that he or she may then apply under certain circumstances to the Connecticut Commissioner of Consumer Protection for an order directing payment out of the above referenced account for the amount unpaid upon the judgment.

96. As set forth above, Quagliani and each of the Class Members suffered damage due to Equifax's failure to maintain their social security numbers in the manner described in C.G.S. §§ 42-470 *et seq.* and as such, Quagliani and each of the Class Member claims such damages and other relief as might be available to them in an amount to be proven at trial.

97. Because of the failure of Equifax to safeguard the 3I of its customers, Equifax is subject to the imposition of civil penalties for each offense against Quagliani and each Class Member, with actual damages to be established at trial.

**FOURTH CLAIM FOR RELIEF: FAILURE TO PROVIDE TIMELY NOTIFICATION OF DATA BREACH AS IS REQUIRED BY C.G.S. §§ 36a-701b AND 38a-999b**

98. Plaintiffs incorporate by reference paragraphs numbered 1 to 97 of the Complaint as fully as if set forth herein.

99. Defendant Equifax, Inc. d/b/a Equifax Healthcare Services is a "company" within the meaning of C.G.S. § 38a-999b in that it is, upon information and belief, a healthcare "utilization review company" as that phrase is defined in C.G.S. § 38a-591a.

100. Defendant Equifax is also a "credit rating agency" within the meaning of C.G.S. §§ 36a-695(4) and 36a-701(2).

101. By virtue of the foregoing, Equifax, both in its capacity as a credit rating agency and in its capacity doing business as a healthcare "utilization review company" under the trade name of Equifax Healthcare Services, are "persons" within the meaning of C.G.S. §§ 36a-701b(b)(1).

102. As such, Equifax was required to provide timely notice of the Data Breach that caused the release of the Plaintiff's and each Class Member's "personal information" -- within a reasonable time after discovery and in the manner provided for under Section 701b -- as is statutorily required by C.G.S. §§ 36a-701b and 38a-999b.

103. Upon information and belief, Equifax purposefully failed to timely provide the public or the Plaintiff and Class Members with notice of the Data Breach for all the reasons previously described.

104. The Plaintiff and Class Members request a declaration that Equifax's failure to comply with the above referenced statutory notification requirements is contrary to Connecticut public policy, is immoral and unethical, and further constitutes a violation of CUTPA as is expressly provided for in C.G.S. § 36a-701b(g).

**FIFTH CLAIM FOR RELIEF: UNFAIR TRADE PRACTICES IN VIOLATION OF C.G.S. § 42-110b**

105. Plaintiffs incorporates by reference all preceding paragraphs numbered 1 to 104 as if fully set forth herein.

106. The acts and practices alleged herein occurred in the course of Equifax conducting "trade" and "commerce" in the State of Connecticut within the meaning of C.G.S § 42-110a(4).

107. The Data Breach, which compromised the personal information, including social

security numbers, of Connecticut citizens constitutes a “breach of security,” as that term is defined by C.G.S. § 36a-701b(a) and is further a violation of C.G.S. § 42-470 *et seq.*

108. In the manner described herein, Equifax unreasonably delayed disclosing the Data Breach to the Class within a reasonable time after its discovery as was required by C.G.S §§ 36a-701b(b) and 38a-999b.

109. Additionally, upon information and belief, Equifax not only failed to disclose the Data Breach within a reasonable time, but Equifax's failure to do so was intentional. Equifax purposefully concealed as long as possible the massive scale of the Data Breach from consumers, both to try and hide Equifax's gross negligence and willful disregard for the welfare of consumers, as well as to facilitate certain members of Equifax's management engaging in insider trading activities by offloading their Equifax stock to unsuspecting buyers before the news of the cataclysmic nature of the damages that Equifax had caused to almost half of the U.S. population became generally known.

110. Pursuant to C.G.S. § 36a-701b(g), Equifax's failure to disclose the Data Breach following the discovery thereof in March 2017 within in a reasonable time period to each Connecticut resident whose 3I was, or was reasonably believed to have been, accessed by an unauthorized person through the Data Breach constitutes unfair and/or deceptive acts or practices. C.G.S. § 42-110b.

111. Equifax's various acts of concealment of the Data Breach, including post-notification, ongoing concealment, and misrepresentations, are immoral, unethical, against public policy, and constitute unfair and deceptive trade practices in violation of CUTPA.

112. Equifax engaged in the unfair acts or practices alleged herein willfully when it knew or should have known that its conduct was unfair in violation of C.G.S. § 42-110b and

therefore, Defendants are liable for civil penalties of up to \$5,000 per willful violation pursuant to C.G.S. § 42-110(b).

113. Quagliani and the Class Members have suffered an ascertainable loss of money or property, real or personal, as a result of Equifax's above referenced actions in violation of CUTPA, and are entitled to recover their actual damages, as well as in in the Court's discretion, an award of punitive damages and such equitable relief as the Court may deem just, equitable and proper all as provided for in C.G.S § 42-110g.

114. Quagliani and the Class Members are expressly authorized to proceed as a class pursuant to C.G.S. § 42-110g(b) to bring this claim as a class action to recover damages for the benefit of affected residents of Connecticut injured in this state by Equifax's CUTPA violations.

115. A copy of this complaint will be mailed to the Connecticut Attorney General and the Commissioner of Consumer Protection as required by C.G.S. § 42-110g(c).

116. Plaintiff further claims a right to an award of its reasonable attorneys' fees and equitable relief under C.G.S. § 42-110g(d).

**SIXTH CLAIM FOR RELIEF: COMMON LAW NEGLIGENCE**

117. Plaintiff and Class Members repeat and reallege the allegations of paragraphs 1 to 117 of the Complaint as fully as if set forth herein.

118. Equifax owed Quagliani and the Class Members a duty to use reasonable care to safeguard their most sensitive and private personal financial information (*i.e.*, 3I), *inter alia*, as it was plainly foreseeable to Equifax that its failure to take reasonable precautions to safeguard the public's 3I would expose Quagliani and the Class Members (as well as potentially the entire U.S. population) to massive, permanent, and nearly irreparable financial harm.

119. Equifax's duty was only further heightened after Equifax was put on advance



notice as to a specific and imminent threat that could have been easily stopped had Equifax bothered to expend even a small modicum of corrective effort.

120. The Data Breach was a direct and proximate result of Equifax's negligence.

121. Quagliani and the Class Members have been severely and permanently injured as a result of Equifax's above referenced negligence and claim damages in an amount to be proven at trial.

122. Equifax's above described actions were outrageous, and evidence a reckless indifference to and a wanton violation of the 3I privacy rights of Quagliani and the Class Members entitling Quagliani and the Class Members to an award of punitive damages.

**DEMAND FOR RELIEF**

WHEREFORE, Plaintiff demands judgment, on behalf of herself individually and as

Representative of the Class, as follows:

- a. That this action proceed as a class action with Quagliani serving as the Class Representative, and with Quagliani's counsel as Class Counsel, and that judgment be entered in favor of Quagliani and the Class;
- b. Declaring and otherwise finding that the Defendants have violated the Fair Credit Reporting Act (the "FCRA"), as well as C.G.S. §§ 42-470 *et seq.*, 36a701b and the Connecticut Unfair Trade Practices Act, C.G.S. §42-110b ("CUTPA").
- c. Awarding the Plaintiff statutory damages for Defendants' violations of the FCRA, 15 U.S.C. §§ 1681n and 1681o, and actual damages in an amount to be proven at trial;
- d. Enjoining the Defendants from continuing the unfair acts or practices as complained of herein under Connecticut state law, C.G.S §§36a-701b, 42-471, 42-110, and ordering any further or different mandatory injunctive relief the Court deems just, equitable and proper.
- e. An order, pursuant to C.G.S. §42-110(b), directing defendants to pay civil penalties of not more than \$5,000 for each willful violation of C.G.S. §42-110b(a), plus any applicable fines and civil penalties provided for under C.G.S. § 42-470 *et seq.*.
- f. Awarding Plaintiffs their reasonable attorneys' fees, disbursements and costs as provided for under the FCRA (15 U.S.C. § 1681n and 1681o) and CUTPA (C.G.S. § 42-110g).
- g. Punitive damages for any proven violations by Defendants of either the FCRA (15 U.S.C. § 1681n) or CUTPA (C.G.S. § 42-110g).
- h. Compensatory and punitive damages caused by Defendants' negligence.
- i. Prejudgment and post-judgment interest to the extent allowable under applicable law.
- j. That the Equifax Defendants be ordered to either free credit monitoring or credit repair services for the remainder of the natural lives of Plaintiff and the Class through a funding mechanism to be created in this action.
- k. That the Equifax Defendants be responsible financially for the costs and expenses of a Court approved notice program through pst and media designed to give immediate notification to the Class;

1. Such other and further relief as this Court may deem just and proper.

Respectfully submitted,

THE PLAINTIFF  
NATALIE QUAGLIANI,  
INDIVIDUALLY AND AS CLASS  
REPRESENTATIVE

By:                           /S/                            
Steven J. Moore (ct07063)  
James Nealon (ct08161)  
WITHERS BERGMAN LLP  
1700 East Putnam Avenue  
Greenwich, Connecticut 06850  
Ph: (203) 302-4100  
Fax: (203) 302-868-0558  
Email: [steven.moore@withersworldwide.com](mailto:steven.moore@withersworldwide.com)