UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

GARY CAMPBELL, individually and on behalf all others similarly situated,

Plaintiff,

EQUIFAX, INC., a Georgia corporation,

Defendant.

Case No.:

CLASS ACTION ON BEHALF OF PLAINTIFF AND ALL OTHERS SIMILARLY SITUATED

COMPLAINT FOR DECLARATORY RELIEF, INJUNCTIVE RELIEF, AND DAMAGES

DEMAND FOR JURY TRIAL

Plaintiff Gary Campbell ("Plaintiff"), individually and on behalf of all other similarly situated consumers of the United States, files this class action complaint against Defendant Equifax, Inc., by and through his undersigned counsel, upon personal knowledge as to facts pertaining to him and on information and belief as to all other matters, brings this action against Equifax, Inc. ("Equifax" or "Defendant"), and states the following:

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

NATURE OF THE ACTION

1. Equifax boasts: "We have built our reputation on our commitment to deliver reliable information to our customers, . . . and to protect the privacy and confidentiality of personal information about consumers. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."

2. This claim on Equifax's "Privacy" webpage remains, even though Equifax's failed data security allowed third parties to access the names, addresses, Social Security numbers, and other personally identifiable information ("PII") of over 145 million United States consumers—almost half the population of the United States.

3. Equifax also admits that credit card numbers for approximately 209,000 United States consumers were accessed, as was dispute documentation (that contained additional PII) for approximately 182,000 Unites States consumers. Since its initial disclosure, Equifax has admitted that credit card transaction history going back to November 2016 was also included for some affected individuals.

4. This data breach ("Breach") purportedly began in mid-May and ended on July 29, 2017, when Equifax finally realized its security had been compromised.

5. While Equifax allegedly learned of the Breach on July 29, 2017, Equifax did not acknowledge the Breach or inform the public until September 7, 2017, well over a month later. This delay, coupled with Equifax's decision to apparently announce the data breach after the end of the trading day (and after several of its executives unloaded some stock worth approximately $2 million),

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

belies Equifax's claim that it began notification as soon as it had enough information to do so.

6. Equifax has since revealed the true cause of the Breach: a patchable vulnerability in the open source software Apache Struts. Equifax claims that it engaged an independent cybersecurity firm to conduct a comprehensive forensic review. Despite that, and despite having five weeks from discovery to public notification, Equifax's initial disclosures were vague, referencing a "U.S. website application vulnerability."[1] Equifax waited an additional week before revealing the root cause of the security breach, which turned out to be entirely preventable.

7. Equifax also acknowledged the following day that it had been aware of the vulnerability and the patch in early March 2017.[2] Equifax could have prevented the Breach entirely had it updated its software when notice of the patch went out in March 2017—some two months before Equifax claims the Breach started.[3]

8. The Breach followed other recent Equifax security breaches that exposed the Social Security numbers and other PII of thousands of individuals. These prior events should have provided Equifax advanced warning of their data security shortcomings, yet Equifax still failed to adequately safeguard consumers' PII, creating a massive threat to those whose PII was improperly safeguarded.

9. Not only that, but, two weeks after its initial disclosure of the Breach, Equifax confirmed that it had experienced yet another security incident earlier in the

---

[1] Cybersecurity Incident & Important Consumer Information (Consumer Notice), Equifax Security 2017, https://www.equifaxsecurity2017.com/consumer-notice/.

[2] Press release, "Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes," Equifax Investor Relations (Sept. 15, 2017), https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832.

[3] Brian Krebs, "Equifax Hackers Stole 200k Credit Card Accounts in One Fell Swoop," KrebsOnSecurity (Sept. 14, 2017), https://krebsonsecurity.com/2017/09/equifax-hackers-stole-200k-credit-card-accounts-in-one-fell-swoop/

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

year, before the Breach, telling NPR that, "during the 2016 tax season, Equifax experienced a security incident involving a payroll-related service."5 Equifax failed to shore up its security before the Breach despite repeatedly being put on notice that its security was wholly inadequate.[4]

10. Senator Mark Warner (D-Va.), who heads the bipartisan Senate Cybersecurity Caucus, stated that "it is no exaggeration to suggest that a breach such as this – exposing highly sensitive personal and financial information central for identity management and access to credit – represents a real threat to the economic security of Americans."[5]

11. This Complaint is filed on behalf of all persons who were victimized by the Breach, as more fully described herein. As a result of Equifax's willful failure to prevent the Breach, Plaintiff and the Class are far more likely to suffer from identity theft and financial fraud, including fraudulently filed tax returns, fraudulent transactions on existing lines of credit, obtaining government benefits in a victim's name, and the creation of fraudulent financial accounts opened in their names, among myriad other risks. Due to these risks, the victims of the Breach will have to pay for credit monitoring and identity theft protection services far more than a year into the future, and many will seek such services from a company other than the one that exposed their information in the first place. Ultimately, victims of the Equifax

---

[4] Merrit Kennedy, "Equifax Confirms Another 'Security Incident,'" NPR (Sept. 19, 2017, 9:46 p.m.), http://www.npr.org/sections/thetwo-way/2017/09/19/552124551/equifax-confirms-anothersecurity-incident; see also Michael Riley, Anita Sharpe, and Jordan Robertson, "Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed," Bloomberg Technology (Sept. 18, 2017, 2:55 p.m.), https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed ("The revelation of a March breach will complicate the company's efforts to explain a series of unusual stock sales by Equifax executives.").

[5] Lee Mathews, "Equifax Data Breach Impacts 143 Million Americans," Forbes (Sept. 7, 2017, 10:42 p.m.), https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#4893c931356f.

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

breach have devoted and will continue to devote significant time, money, and energy into safeguarding and monitoring their PII and accounts linked to it for years to come.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action 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 million exclusive of interest and costs, and many members of the Class, including Plaintiff, are citizens of different states than Defendant.

13. This Court has personal jurisdiction over Defendant because Defendant has sufficient minimum contacts with the State of Washington and/or Defendant otherwise purposely avails itself of the markets in Washington by conducting consumer reporting and monitoring services in Washington and advertising in Washington. Defendant's purposeful availment of the markets in Washington renders the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

14. Venue is proper in this judicial district pursuant to 28 U.S.C. §1391 because Equifax regularly conducts business in this district, unlawful acts or omissions are alleged to have occurred in this district, and Equifax is subject to personal jurisdiction in this district.

PARTIES

15. Plaintiff Gary Campbell is a resident of Battle Ground, Clark County, Washington. As confirmed by Equifax, Plaintiff's PII and/or credit account

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

information was included in the Data Breach and was disclosed to unauthorized third parties and, therefore, was harmed as a direct and proximate result thereof.

16. As a direct and proximate result of Defendant Equifax's wrongful acts or omissions (as set forth fully herein) and the resulting data breach, Plaintiff and each of the Class members have suffered actual harm and have been placed at imminent substantial and continuing risk for identity theft or identity fraud (as Equifax has conceded in its recent press releases and by its creation of a urging consumers to sign up for credit file monitoring and identity theft protection).

17. As a direct and proximate result of Defendant Equifax's wrongful acts or omissions and the resulting Data Breach, Plaintiff and each Class member have spent time, and will continue to spend time and effort in the future, monitoring their financial accounts. Additionally, the PII and/or credit account information of Plaintiff and each Class member has been placed at a substantially increased risk of identity fraud/theft or other misuse, thus requiring them to take protective measures they would not have had to take but for the Data Breach. Any additional misuse of Plaintiff's or the Class members' PII or credit account information will result in additional damages.

18. Defendant Equifax is a Georgia corporation with its headquarters in Atlanta, Georgia.

FACTUAL ALLEGATIONS

19. On September 7, 2017, Equifax announced that it had suffered a breach that exposed the names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers for over 140 million United States consumers. In addition, Equifax admitted that credit card numbers for approximately

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

209,000 customers were breached, and dispute documentation for approximately 182,000 customers was also accessed, which included additional PII.

20. Equifax claims that it discovered the Breach on July 29, 2017. Equifax claims that the Breach began in mid-May 2017, and remained undetected for almost three months until Equifax's alleged discovery on July 29.

21. After discovery, Equifax waited over a month before disclosing the Breach. While Equifax claims it began notification as soon as it had enough information to do so, its preparations left 143 million consumers with their most sensitive information exposed.

22. Perhaps more troubling is that Equifax executives, including the Equifax Chief Financial Officer, the President of U.S. Information Solutions, and the President of Workforce Solutions, made unscheduled transactions selling hundreds of thousands of dollars in Equifax stock mere days after the Breach was discovered, but about a month before Equifax made the news public. For example, John Gamble, Equifax's Chief Financial Officer, sold shares worth over $946,000. Yet, Equifax has claimed that these high-level executives had no knowledge of the breach.

23. On September 13, 2017, Equifax confirmed what security researchers already suspected in an update to its breach disclosure:

> Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638.[6]

24. Apache Struts is a popular open source framework used to develop Java-based apps. Its users include governmental agencies, Fortune 500 companies, Experian (another credit reporting agency), and

---

[6] "A Progress Update for Consumers, Equifax Security 2017 (Sept. 13, 2017), https://www.equifaxsecurity2017.com/2017/09/13/progress-update-consumers-4/.

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

annualcreditreport.com, the website provided for by the federal government for annual free credit checks.

25. Troublingly, the vulnerability Apache Struts CVE-2017-5638 was detected— and patched—months before Equifax alleges the Breach began. Security researchers identified the so-called "zero day" vulnerability in early March 2017. Apache Struts had released a patch by March 8, 2017.[7] The National Vulnerability Database, hosted by the U.S. National Institute of Standards and Technology, had a detailed page on the vulnerability posted on March 10, 2017, with links to analysis and patch information.[8]

26. The patch was provided free of charge, and security researchers went to great lengths to publicize it. All Equifax had to do was update its systems, which it failed to do.

27. Had Equifax properly deployed the patch when it was first released, it is likely the Breach would have been prevented.

28. As one of the three largest credit bureaus in the United States, Equifax is believed to have PII in its possession on over 800 million individuals worldwide. Equifax's business model revolves around buying, selling, collecting, and storing consumers' PII for financial gain.

29. Due to Equifax's relatively unique position as a purveyor of such a massive amount of PII, Equifax also owns and operates a number of credit-related

---

[7] Brian Krebs, "Equifax Hackers Stole 200k Credit Card Accounts in One Fell Swoop," KrebsOnSecurity (Sept. 14, 2017), https://krebsonsecurity.com/2017/09/equifax-hackers-stole-200k-credit-card-accounts-in-one-fell-swoop/. Screenshots for both annualcreditreport.com and Experian, showing the vulnerability, were publicly posted the same week.

[8] "CVE-2017-5638 Detail," National Vulnerability Database (original release March 10, 2017; last revised August 15, 2017), https://nvd.nist.gov/vuln/detail/CVE-2017-5638.

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

services, including an identity theft protection and credit monitoring service, called TrustedID, which uses Equifax's vast PII database to attempt to monitor for fraud.

30. The other two major credit bureaus, Experian and Transunion, have similar services, called ProtectMyID and TrueIdentity, respectively. Due to the nature of their business, these larger credit bureaus know, or have every reason to know, the value of the PII they possess, and the importance of creating safeguards to protect consumers' PII from exposure and misuse.

31. PII is valuable and thus is a frequent target of hackers. As such, in recent years many large companies and aggregators of PII have suffered data breaches, including Adobe, LinkedIn, eHarmony, MySpace, Snapchat, Friend Finder Network, Anthem, and Yahoo (multiple times), among others.

32. These breaches were extremely well-publicized, and should have put Equifax on alert to the prevalence of such breaches and that formidable data security policies and practices were warranted.

33. Equifax has had every reason to know of the risks associated with—and value of—stored PII. In the wake of some of the breaches listed above, the companies at fault would sometimes turn to Equifax to provide credit monitoring services to the harmed individuals.

34. Further, Equifax itself suffered data breaches as recently as May 2016 and March 2017, when W-2 forms for thousands of employees of the Kroger stores or Allegis Group, Inc., were stolen from other websites operated by Equifax or one of its wholly owned subsidiaries.

35. To put the value of PII into context, the 2013 Norton Report, based on one of the largest consumer cybercrime studies ever conducted, estimated that the

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

global price tag of cybercrime is around $113 billion, with the average cost per victim being $298 dollars.

36. Between being in the business of identity protection, and the multitude of well publicized data breaches, including its own, Equifax had significant notice that it needed to maintain adequate security measures to insure the security of Plaintiff's PII, yet Equifax failed to do so.

37. Equifax failed to take proper precautions before the Breach—the basic act of keeping its web applications up to date—and it appears the Breach and associated reputation damage have not inspired Equifax to change its woeful approach to security.

38. Plaintiff and Class members are at a heightened, imminent risk of identity theft and fraud as result of their PII getting into the hands of malicious third-parties.

39. In response to this heightened, imminent risk of identity theft and fraud, Equifax is offering 12-month subscriptions for a year of its identity theft product, TrustedID Premier.

40. Unfortunately, the TrustedID service being offered is wholly inadequate to address the injuries Plaintiff and Class members have and will face.

41. TrustedID is a wholly owned subsidiary of Equifax that is believed to be operated by Equifax. Given that it was Equifax's flawed data security and practices that led to Plaintiff's injuries in the first place, its TrustedID service does not promote confidence. Plaintiff and Class members must not be asked to trust Equifax to solve the very problem it caused.

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

42. Even if TrustedID were not owned and operated by Equifax, Equifax offers an inadequate and insufficient remedy for its failure to adequately protect and secure Plaintiff's and Class members' PII. The subject service has a history of consumer complaints about its inability to actually detect identity theft, as well as the difficulty in obtaining customer service. Many customers and reviewers have suggested that customer service is only available by phone for limited hours Monday through Friday.

43. Even if TrustedID were an adequate identity protection service, it stands to reason that an influx of half the population of the United States will further degrade the accessibility and quality of identity theft and credit monitoring services of TrustedID, rather than improve them.

44. The limited amount of protection—one year—offered through TrustedID further exacerbates the problem, as many identity thieves will wait years before attempting to use the personal information they have obtained, especially when it comes to Social Security numbers, which are burdensome to change.

45. In particular, a Government Accountability Office ("GAO") study found that "stolen data may be held for up to a year or more before being used to commit identity theft." In order to protect themselves, Plaintiff and Class members will need to remain vigilant against unauthorized data use for years and decades to come.[9]

46. The Breach was the direct and proximate result of the Equifax's failure to properly safeguard Plaintiff's and Class members' PII from exposure as required by state and federal laws and regulations, including the Gramm-Leach-Bliley Act ("GLBA"), among others.

---

[9] "Report to Congressional Requesters," p. 33, Government Accountability Office (June 2007), www.gao.gov/new.items/d07737.pdf.

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

47. Specifically, the GLBA imposes upon "financial institutions" "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." *See* 15 U.S.C. § 6801.

48. For purposes the GLBA, "non-public personal information" means personally identifiable financial information— (i) Provided by a consumer to a financial transaction; (ii) Resulting from any transaction with the consumer or any service performed by the consumer; or (iii) Otherwise obtained by the financial institution. *See* 15 U.S.C. § 6809(4).

49. To satisfy this obligation, financial institutions must satisfy certain standards relating to administrative, technical, and physical safeguards: (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. *See* 15 U.S.C. § 6801(b).

50. In order to satisfy its obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program" that, among other requirements, identifies "reasonably foreseeable internal and external risks to security, confidentiality, and integrity of consumer information that could result in unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks." *See* 16 C.F.R. § 314.4.

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

51. Further, under the Interagency Guidelines Establishing Information Security Standards related to the GLBA, 12 C.F.R. Pt. 225, App. F, financial institutions have an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.*

52. In addition, the Interagency Guidelines provide that "[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible." See 12 C.F.R. Pt. 225, App. F.

53. For purposes of the GLBA, Equifax is a financial institution, and is therefore subject to its provisions. Equifax admits as much in its filings with the Securities and Exchange Commission.[10]

54. For the purposes of the GLBA, Plaintiff's and Class members' PII is both "nonpublic personal information" and "sensitive customer information."

55. If Equifax had developed, implemented, and maintained a comprehensive information security program as required by 16 C.F.R. § 314.4—that is, complied with the law—Plaintiff's and Class members' PII would not have been accessible to unauthorized persons.

---

[10] See Equifax, Inc. 2016 10-K Report, ("We are subject to various GLBA provisions, including rules relating to the use or disclosure of the underlying data and rules relating to the physical, administrative and technological protection of non-public personal financial information."), https://www.sec.gov/Archives/edgar/data/33185/000003318517000008/efx10k20161231.htm.

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

56. Equifax, despite having known of the Breach for more than a month before notifying anyone publicly, put forth a notification site that further confused the issues. Equifax's breach-related site (equifaxsecurity2017.com), where consumers were entering six-digits of their Social Security numbers, had the administrator's credential information publicly available, a simple registration issue that should have been dealt with before the site went live.

57. Astonishingly, in the wake of the Breach, some Equifax customer service representatives have been directing consumers to the wrong website via Twitter, erroneously sending consumers to "securityequifax2017.com" instead of "equifaxsecurity2017.com" and putting them at extreme risk of inputting information into a phishing website run by scammers.[11]

58. Equifax failed to develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems, in violation of 12 C.F.R. Pt. 225, App. F. Equifax also failed to notify affected individuals affected by the Breach whose nonpublic personal information or sensitive customer information was exposed as soon as possible, or in a timely and adequate manner.

59. Ultimately, Plaintiff's and Class members' injuries are a direct and proximate result of Equifax's failure to provide adequate security for Plaintiff's and Class members' PII, and Equifax's violation of applicable state and federal laws and regulations.

CLASS ALLEGATIONS

[11] Dell Cameron, "Equifax Has Been Sending Consumers to a Fake Phishing Site for Almost Two Weeks," Gizmodo (Sept. 20, 2017, 11:03 a.m.), https://gizmodo.com/equifax-has-been-sendingconsumers-to-a-fake-phishing-s-1818588764. Luckily, that particular domain is owned by a good Samaritan who has posted a warning about security and phishing rather than preying on affected consumers.

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

60. Plaintiff brings this action on behalf of himself and the members of the proposed Classes under Rule 23(a), (b)(2), (b)(3), and/or (c)(4) of the Federal Rules of Civil Procedure. Plaintiff seeks to represent the following Classes:

Nationwide Class: All persons in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach publicly announced by Equifax, Inc. on September 7, 2017.

Washington Class: All persons in Washington state whose personally identifiable information was acquired by unauthorized persons in the data breach publicly announced by Equifax, Inc. on September 7, 2017.

61. Except where otherwise noted, "the Class" and "Class members" shall refer to members of the Nationwide Class and the Washington Class, collectively.

62. Plaintiff reserves the right to redefine the Classes prior to class certification, after having the opportunity to conduct discovery and further investigation.

63. Plaintiff reserves the right to establish additional subclasses as appropriate.

64. Excluded from the Classes are Equifax, its parents, subsidiaries, affiliates, officers and directors, and any entity in which Equifax has a controlling interest.

65. **Numerosity**. Fed. R. Civ. P. 23(a)(1). The Class members are so numerous that joinder is impractical. The Classes consist of over 140,000,000 members, the precise number which is within the knowledge of Equifax and can be ascertained by discovery and review of Equifax's records.

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

66. **Commonality**. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are numerous questions of law and fact common to the Class members, which predominate over any questions affecting only individual Class members. Common questions of law and fact include, but are not limited to:

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

b. Whether Equifax owed a duty to Plaintiff and the Class members to adequately protect their PII;

c. Whether Equifax breached its duties to protect the personal information of Plaintiff and Class members;

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

e. Whether Equifax violated the law as alleged herein;

f. Whether Equifax failed to adequately safeguard PII under the Financial Services Modernization Act of 1999, a.k.a. the Gramm-Leach-Bliley Act;

g. Whether Plaintiff and members of the Class are entitled to equitable and declaratory relief, including injunctive relief, and if so, the nature of such relief.

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

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

68. **Typicality**. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and all members of the Class have been injured by the same wrongful, deceptive, and unlawful practices of Equifax and allege similar or the same legal theories.

69. **Adequacy**. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately assert and protect the interests of the Classes, and have retained counsel experienced in prosecuting class actions. Plaintiff has no interests adverse to the interests of the members of the Classes. Accordingly, Plaintiff is an adequate representative and will fairly and adequately protect the interests of the Classes.

70. **Superiority**. Fed. R. Civ. P. 23(b)(3). A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit, because individual litigation of the claims of all Class members is economically unfeasible and procedurally impracticable. While the aggregate damages sustained by Class members are in the millions of dollars, the individual damages incurred by each Class members resulting from Equifax's wrongful conduct do not warrant the expense of individual lawsuits. The likelihood of individual Class members prosecuting separate claims is remote, and, even if every Class member could afford individual litigation, the court system would be unduly burdened by individual litigation of such cases.

71. The prosecution of separate actions by Class members would create a risk of establishing inconsistent rulings and/or incompatible standards of conduct for Equifax. Additionally, individual actions may be dispositive of the interests of the Class, although certain class members are not parties to such actions.

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

72. **Injunctive and Declaratory Relief**. Fed. R. Civ. P. 23(b)(2). The conduct of Equifax is generally applicable to the Classes as a whole and Plaintiff seeks equitable remedies with respect to the Classes as a whole. As such, the policies and practices of Equifax make declaratory or equitable relief with respect to the Classes as a whole appropriate.

73. **Issue Certification**. Fed. R. Civ. P. 23(c)(4). In the alternative, the common questions of law and fact, set forth above, are appropriate for issue certification on behalf of the Classes.

FIRST CAUSE OF ACTION

Violation of the Washington Consumer Protection Act

74. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

75. Plaintiff and Washington Class members' PII was in the possession of Equifax at the time of the Breach.

76. Washington's Consumer Protection Act, RCW §§ 19.86.010, *et seq.* ("CPA"), protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

77. To achieve that goal, the CPA prohibits any person from using "unfair methods of competition or unfair or deceptive acts or practices in the conduct of any trade or commerce. . . ." RCW § 19.86.020.

78. Defendant expressly represented that it would safeguard and protect PII. Defendant made these representations available to the Washington Class at all times (including through its website).

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

79. Consistent with its representations, Defendant accepted responsibility for securing Plaintiff's and the Washington Class members' PII. Given that it was Defendant's responsibility for creating, overseeing, maintaining, and otherwise implementing its own data security practices, Defendant knew (or should have known) that it was not adequately protecting Plaintiff's or the Washington Class Members' PII in accordance with its express guarantees. This is particularly true given the many warning signs that Defendant's systems were at risk of a breach.

80. Despite this knowledge, Defendant failed to disclose that its data security systems and practices did not comport with the express representations set forth above, and otherwise described herein. In sum, Defendant did not disclose that it did not take appropriate steps to secure electronic systems from unauthorized use, did not ensure that authorized personal had access to PII only to the extent necessary to conduct their business, and did not meet its obligations under state and federal laws. Instead, Defendant continued to represent that its data security system was secure, even though it knew (or should have known) that it was not.

81. Defendant's conduct was deceptive. By failing to honestly disclose its true data security practices at the time that it accepted and maintained the PII of Plaintiff and the Washington Class, Defendant made affirmative misrepresentations and, thus, engaged in deceptive acts or practices.

82. Given that Defendant alone knew about the true state of its data security and privacy practices, Defendant purposefully used its inflated representations of data security and privacy protocols, which it knew were false at the time they were made to consumers, to mislead Plaintiff into believing his PII was

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

safe. Defendant's conduct therefore had the capacity to deceive a substantial portion of the public.

83. Prior to Defendant's public announcement of the data breach, neither Plaintiff, nor members of the Washington Class, nor the general public could have known that Defendant was not implementing the data security and privacy protocols in accordance with its own consumer-facing representations and applicable duties. Rather than implement the data security and privacy protocols it promised-including by timely notifying Plaintiff and the Washington Class promptly about the data breach-Defendant actively concealed its true practices and protocols.

84. Defendant's conduct was also unfair. Defendant engaged in unfair acts or practices by making the data security representations discussed, which it did to assure Plaintiff and the Washington Class, who were concerned about the privacy and security of their PII, that their PII would be safe.

85. Defendant, however, failed to make good on its promises of data security by not investing the necessary resources in its cybersecurity program, not promptly notifying Plaintiff and the Washington promptly about the data breach, and otherwise not living up to the specific representations and obligations set forth above. Given the known risk of maintaining PII with relaxed cybersecurity practices, Defendant's conduct was likely to cause substantial injuries to consumers.

86. As set out above, because only Defendant knew (or should have known) that it was not complying with its own data security representations and obligations, there was no way for members of the public, including Plaintiff and members of the Washington, to avoid the injury caused by Defendant's conduct.

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

87. Consumers, like Plaintiff and members of the Washington Class, value their privacy. Companies such as Defendant that offer adequate data security protections are more valuable to consumers than those with substandard security practices.

88. Based on the representations made by Defendant, Plaintiff and the Washington Class members believed Defendant would adequately protect their PII and those security protections were valuable to them. Accordingly, Defendant's omission regarding its true protection practices was material.

89. Had Plaintiff and members of the Washington Class known that Defendant did not actually implement its promised data security and privacy protocols, they would not have been willing to provide Defendant with their PII.

90. Defendant's failure to disclose its actual (and substandard) security practices substantially injured the public because it caused millions of consumers' PII to be compromised. Further, Defendant's use of substandard security did not create any benefits sufficient to outweigh the harm it caused.

91. Defendant's deceptive and unfair acts or practices occurred in its trade or business and has proximately caused injury to Plaintiff and the putative Washington Class. Defendant's general course of conduct is injurious to the public interest, and such acts are ongoing and/or have a substantial likelihood of being repeated inasmuch as the long-lasting harmful effects of its misconduct may last for years (e.g., affected individuals could experience identity theft for years). As a direct and proximate result of Defendant's unfair acts, Plaintiff and members of the Washington Class have suffered actual injuries, including without limitation investing

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

substantial time or money in monitoring and remediating the harm inflicted upon them.

92. As a result of Defendant's conduct, Plaintiff and members of the Washington Class have suffered actual damages, including the lost value of their privacy, the lost value of their personal data and lost property in the form of their breached and compromised PII (which is of great value to third parties); ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

93. With respect to injunctive relief, Plaintiff, on behalf of himself and members of the Washington Class, seek an Order requiring Defendant to: (1) engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to correct any problems or issues detected by such third-party security auditors promptly; (2) engage third-party security auditors and internal personnel to run automated security monitoring; (3) audit, test, and train its security personnel regarding any new or modified procedures; (4) segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

network is compromised, hackers cannot gain access to other portions of Defendant; (5) curing checks; (6) routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (7) meaningfully educate all class members about the threats they face as a result of the loss of their confidential financial, personal, and health information to third parties, as well as the steps affected individuals must take to protect themselves.

SECOND CAUSE OF ACTION

Violation of Washington Data Breach Disclosure Law

94. Plaintiff incorporates all the foregoing factual allegations as if fully set forth herein.

95. Plaintiff alleges additionally and alternatively that RCW 19.255.010(2) provides that "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." *See* RCW 19.255.010(2) (2005).

96. The breach resulted in an "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendant and, therefore, experienced a "breach of [its] security of [its] system", as defined by RCW 19.255.010(4) (2005).

97. Defendant failed to disclose the breach of its network immediately, after discovering the breach. Instead, it waited months before notifying all affected

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 6th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

individuals. Defendant unreasonably delayed informing Plaintiff and members of the Washington Class about the data breach after it knew or should have known that the data breach had occurred.

98. Defendant's failure to provide notice immediately after discovering the breach is a violation of RCW 19.255.010.

THIRD CAUSE OF ACTION

Negligence

99. Plaintiff incorporates all the foregoing factual allegations as if fully set forth herein.

100. Plaintiff alleges additionally and alternatively that by collecting and storing PII, Defendant had a duty of care to use reasonable means to secure and safeguard this information, to prevent disclosure of the information, and to guard the information from theft. Defendant's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give immediate notice in the case of a data breach.

101. Furthermore, given the other major data breaches affecting Defendant and other industries, and that the vulnerabilities Defendant knew (or should have known about) could be exploited by hackers and expose PII, Plaintiff and the Nationwide Class members or alternatively, members of the Washington Class, are part of a well-defined, foreseeable, finite, and discernible group that was at high risk of having their PII stolen.

102. Defendant owed a duty to Plaintiff and members of the Nationwide Class or alternatively, members of the Washington Class, to provide security consistent with industry standards, statutory requirements, and the other

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

requirements discussed herein, and to ensure that its systems and networks—and the personnel responsible for them—adequately protected its consumers' PII.

103. Defendant admitted and assumed its duty to implement reasonable security measures as a result of its general conduct, internal policies and procedures, and outward representations to Plaintiff and Class Members. Through these and other statements, Defendant specifically assumed the duty to comply with industry standards and in protecting PII.

104. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and the Plaintiff and the members of the Nationwide Class or alternatively, members of the Washington Class. The special relationship arose because Plaintiff and the Class Members entrusted Defendant with their PII. Only Defendant was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiff and the members of the Nationwide Class or alternatively, members of the Washington Class, from a data breach.

105. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the common law and the statutes and regulations described above, but also because it was bound by, and had committed to comply with, industry standards for the protection of PII.

106. Defendant breached its common law, statutory and other duties—and thus, was negligent—by failing to use reasonable measures to protect consumers' confidential data from hackers and by failing to provide timely notice of the at-issue breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and proposed Class Members' PII;

b. Failing to monitor the security of its networks adequately;

c. Allowing unauthorized access to Plaintiff's and the proposed Class Members' PII;

d. Failing to recognize in a timely manner that Plaintiff's and proposed Class Members' PII had been compromised; and

e. Failing to warn Plaintiff and Class Members in a timely manner that their PII was likely to be and had been compromised.

107. It was foreseeable that Defendant's failure to use reasonable measures to protect confidential data, to disclose to Plaintiff its inadequate security system, and to provide timely notice of a breach of such data would result in injury to Plaintiff and the members of the Nationwide Class or alternatively, members of the Washington Class. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Nationwide Class or alternatively, members of the Washington Class were reasonably foreseeable, particularly in light of the other major data breaches described herein, which informed Defendant that its network-security procedures were inadequate and that their vulnerabilities could be exploited by hackers to expose PII.

108. It was therefore reasonably foreseeable that the failure to adequately safeguard confidential data would result in one or more of the following injuries to Plaintiff and the members of the proposed Nationwide Class or alternatively, members of the Washington Class: ongoing, imminent, certainly impending threat of

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 | fax 206-340-1962
www.PivotalLawGroup.com

identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

109. Accordingly, Plaintiff, on behalf of himself and members of the Nationwide Class or alternatively, members of the Washington Class, seek an order declaring that Defendant's conduct constitutes negligence, and awarding them damages in an amount to be determined at trial.

FOURTH CAUSE OF ACTION

Constructive Fraud

110. Plaintiff incorporates all the foregoing factual allegations as if fully set forth herein.

111. Defendant 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.

112. As a consumer reporting agency to whom Plaintiff's and Class Members' most intimate, sensitive and private personal information and PII was provided, Defendant 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

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

expected Defendant would adhere to its obligations to adequately protect the sensitive, personal information they provided including the PII Defendant allowed to be stolen.

113. Defendant 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.

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

DEMAND FOR JURY TRIAL

115. Plaintiff hereby demands a jury trial on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and consumers similarly situated, prays for judgment as follows:

A. An Order certifying the proposed Classes defined herein, designating Plaintiff as representative of said Classes, and appointing the undersigned counsel as Class Counsel;

B. For restitution of all amounts obtained by Equifax as a result of its wrongful conduct in an amount according to proof at trial, plus prejudgment and post-judgment interest thereon;

C. For all recoverable compensatory, consequential, actual, and/or statutory damages in the maximum amount permitted by law;

D. For punitive and exemplary damages;

E. For other equitable relief;

PIVOTAL LAW GROUP
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
phone 206-340-2008 I fax 206-340-1962
www.PivotalLawGroup.com

F. For such injunctive relief, declaratory relief, orders, or judgment as necessary and appropriate to prevent these acts and practices;

G. For payment of attorneys' fees and costs as allowable by law; and

H. For all such other relief as this Honorable Court deems appropriate.

DATED this 3rd day of November, 2017

PIVOTAL LAW GROUP, PLLC

Christopher L. Thayer, WSBA #23609
McKean J. Evans, WSBA # 52750
Counsel for Plaintiff and the Proposed Classes
IBM Building, Suite 1217
1200 5th Avenue, Seattle, WA 98101
Phone: (206) 340-2008
Fax: (206) 340-1962
Email: CThayer@PivotalLawGroup.com
MEvans@PivotalLawGroup.com