

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

DORI M. MASHBURN, SARAH L.
HARDY, RICHARD GAINEY,
VALERIE GAINEY, JONATHAN C.
ENTSMINGER, CARRIE L.
ENTSMINGER, JACKIE L. KIER,
ALOHA KIER, LARRY NEWCOMER,
and ANDREA SHAFRAN, individually
and on behalf of all others similarly
situated,

Plaintiffs,

v.

EQUIFAX, INC.,

Defendant.

CIVIL ACTION

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	PARTIES	3
A.	Plaintiffs	3
B.	Defendant	4
III.	JURISDICTION AND VENUE	5
IV.	FACTUAL ALLEGATIONS	6
A.	Equifax Was Negligent in Its Efforts to Protect Highly Valuable Personal Information.....	6
B.	Equifax Failed to Release News of the Massive Breach Within a Timely Manner, and Its Response Has Been Deeply Flawed.....	10
C.	Equifax’s Failures Have Harmed and Will Continue to Harm Breach Victims	16
V.	CLASS ACTION ALLEGATIONS	19
A.	Class Definition(s).....	19
1.	National Class	19
2.	Statewide Classes	20
VI.	CLAIMS FOR RELIEF	23
	COUNT I — Willful Violation of The Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq.	23
1.	Overview	23

2.	Violations of 15 U.S.C. § 1681e(a) – Willful Failure to Maintain Reasonable Security Measures	25
3.	Violations of 15 U.S.C. § 1681b(a) – Furnishing Consumer Data Without a Permissible Purpose	27
4.	Violations of 15 U.S.C. § 1681b(g) – Willful Disclosure of Confidential Medical Data	29
5.	Violations of 15 U.S.C. § 1681c-1 – Willful Failure to Respond to Suspected Identify Theft	30
6.	Plaintiffs and the Nationwide Class Suffered Damages as a Proximate Result of Equifax’s Willful Violations of FCRA and are Entitled to Relief	31
COUNT II — Negligent Violation of the Fair Credit Reporting Act		33
COUNT III — Negligence		38
COUNT IV — Negligence Per Se.....		42
COUNT V — Declaratory Judgment		49
COUNT VI — Violation of the Washington Data Breach Notice Act, Wash. Rev. Code. §§ 19.255.10, et seq.		52
COUNT VII — Violation of Washington Consumer Protection Act, Wash. Rev. Code §§ 19.86.020, et seq.....		54
COUNT VIII — Violation of the Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110, et seq.....		56
COUNT IX — Violation of the Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), and (iv) and (9)(i), et seq.....		59

COUNT X — Violation of the North Carolina Unfair Trade Practices Act	N.C.G.S.A. § 75-1.1(a), et seq.;.....	62
COUNT XI — Violation of the Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602;		65
COUNT XII — Violation of the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), et seq.;		67
COUNT XIII — Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. § 201-1, et seq.		70
VII. PRAYER FOR RELIEF		73
VIII. DEMAND FOR JURY TRIAL		75

PLAINTIFFS' CLASS ACTION COMPLAINT

Plaintiffs bring this action on behalf of themselves and all others similarly situated, against Equifax, Inc. ("Defendant"). Plaintiffs allege the following based upon information and belief, the investigation of counsel, and personal knowledge as to the factual allegations pertaining to himself/herself.

I. INTRODUCTION

1. Equifax, one of the nation's three large credit reporting agencies, trades in the personal information of tens of millions of Americans. Those who trust that information to Equifax have a right to expect that it uses the best possible information security infrastructure and practices. Unfortunately for nearly half of the nation's population, that appears not to have been the case.

2. On September 7th, Equifax disclosed that it had experienced a data breach that has exposed the most sensitive identifying information of 143 million Americans (the "Data Breach"). Equifax later increased that number to 145.5 million. The sensitive identifying information breached includes names, dates of birth, and Social Security numbers: the essential raw materials for identity thieves. The breach also exposed phone numbers, credit card numbers, and nearly 11 million driver's license numbers.

3. The Data Breach does not appear to have been technically sophisticated. Rather, hackers were able to gain access through a common web application with a known vulnerability that reportedly was not properly secured.

4. Once the hackers had access, they had months to search for and obtain the most valuable information for identity thieves before Equifax discovered the breach. Although Equifax knew about the breach for months, it did not tell the tens of millions of victims of that breach until September 7th. And Equifax's response since then has been, to put it charitably, bumbling. Equifax's Chairman and CEO Richard F. Smith announced his retirement following the Data Breach.

5. As a result of Equifax's negligence, tens of millions of Americans are now at increased risk of financial account fraud, tax fraud, and other forms identity theft. That increased risk will last for years, because the non-changeable identifying information has absolutely no expiration date.

6. To redress that and other harms caused by what is already being called the worst consumer data breach in history, Plaintiffs brings this action on behalf of themselves and a proposed nationwide class of similarly situated victims, seeking all available remedies.

II. PARTIES

A. Plaintiffs

1. Class representative Dori M. Mashburn is a U.S. Citizen and resident of King County, Washington. Ms. Mashburn's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

2. Class representative Sarah L. Hardy is a U.S. Citizen and resident of Litchfield County, Connecticut. Ms. Hardy's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

3. Class representatives Richard Gainey and Valerie Gainey are U.S. Citizens and residents of Baltimore, County, Maryland. Mr. Gainey's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law. Likewise, Ms. Gainey's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

4. Class representatives Jonathan C. Entsminger and Carrie L. Entsminger are U.S. Citizens and residents of Guilford County, North Carolina. Mr. and Mrs. Entsminger's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

5. Class representatives Jackie L. Kier and Aloha Kier are U.S. Citizens and residents of Dundy County, Nebraska. Both plaintiffs' data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

6. Class representatives Larry Newcomer and Andrea Shafran are U.S. Citizens and residents of Westmoreland County, Pennsylvania. Mr. Newcomer's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law. Likewise, Ms. Shafran's data was compromised, damaged, and otherwise put at risk by Equifax's gross negligence and other violations of law.

B. Defendant

7. Equifax Inc. is a global company headquartered in Atlanta, Georgia that does business throughout the country and is one of the three primary credit reporting agencies in the United States. Equifax maintains data on more than 820 million consumers worldwide. The company employs approximately 9,900 people and operates or has investments in 24 countries in North America, Central and South America, Europe and the Asia Pacific region. Among Equifax's subsidiaries is Equifax Information Services, LLC, which collects and reports consumer information to financial institutions

III. JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 based on the federal statutory claims below, and the Court has supplemental jurisdiction over Plaintiffs' state law claims under 28 U.S.C. § 1367.

9. This Court also has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because at least one Class member is of diverse citizenship from one defendant, there are 100 or more Class members nationwide, and the aggregate amount in controversy exceeds \$5,000,000.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(3) because the Court has personal jurisdiction over Defendant, a substantial portion of the alleged wrongdoing occurred in this District and Georgia, and Defendant has sufficient contacts with this District and Georgia.

11. Venue is proper in the Northern District of Georgia pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims at issue in this Complaint arose in this District.

IV. FACTUAL ALLEGATIONS

A. Equifax Was Negligent in Its Efforts to Protect Highly Valuable Personal Information

12. Equifax is one of the largest credit reporting agencies in the world. It profits by reporting on people's most sensitive financial information, and touts its "commitment to . . . protect the privacy and confidentiality of personal information about consumers." Hackers gained access to the personal information Equifax pledged to protect not as a result of a complex attack; rather, they exploited a known flaw in a common open-source web development software.

13. The hackers, according to the company, "exploited a U.S. website application vulnerability to gain access to certain files." This vulnerability is a part of a software package for building web applications called Apache Struts. Apache reported the bug in March. Although Equifax was aware of the vulnerability, it failed to patch all its systems with a security update, even though hackers were already taking advantage of that vulnerability elsewhere at that time. As the former CEO Equifax testified in Congress, "the vulnerable version of Apache Struts within Equifax was not identified or patched in response to [an] internal March 9 notification to information technology personnel." Equifax's scans of its systems also failed to detect the vulnerability. As a result, the CEO said, "the vulnerability remained in an Equifax web application much longer than it should have."

14. For more than four months, Equifax left open a known vulnerability that hackers could easily exploit to access the private data of almost half of all Americans. Once hackers exploited the Apache Struts vulnerability they installed a backdoor to Equifax's systems and "roamed undetected in Equifax Inc.'s computer network for more than four months before its security team uncovered the massive data breach[.]" The hackers "accessed dozens of sensitive databases and created more than 30 separate entry points into Equifax's computer systems" before they were discovered on July 29. Equifax acknowledges that for more than two months—from May 13 to July 30—hackers used the Apache Struts vulnerability to "access sensitive information," and that "Equifax's security tools did not detect this illegal access."

15. Equifax's failure to patch a known vulnerability is contrary to its public representations about its data security and in violation of its duty to protect the public's credit data.

16. Equifax has represented that it is a "trusted steward of credit data" and had sufficient information security to protect that data:

Why use Equifax

As the needs of our customers have evolved, so have we. Expanding on our role as the trusted steward of credit data, Equifax has grown into the leading provider of technology-and analytics-fueled information solutions.

17. In a 2011 report, “Leading With Integrity: The Equifax Business Ethics and Compliance Program,” Equifax explained that the Gramm-Leach-Bliley Act required financial institutions to “develop and maintain an information security program to protect the security, confidentiality and integrity of the information.” The report also represented that “Equifax entities that receive and collect consumer and customer information have developed and maintain appropriate information security programs.”

18. Nonetheless, it appears Equifax did not have sufficient infrastructure or procedures to prevent the intrusion. It also appears that Equifax did not have sufficient infrastructure or procedures to detect the intrusion once it occurred. Once the hackers were able to gain access, they appear to have had that access for months, which suggests Equifax had very poor security detection practices.

19.

20. Equifax’s international data security practices suggest the company had a poor information security corporate culture. A group of security researchers

in Argentina recently discovered that Equifax's employee portal to manage credit disputes from customers in that country "was wide open, protected by perhaps the most easy-to-guess password combination ever: 'admin/admin.'" Inside that portal, researchers could reportedly easily discover employee login and password information. Most troubling, the researchers could easily find customers' DNI, the Argentinian equivalent of a Social Security number. "To me, this is just negligence," one of the researchers told Brian Krebs. "In this case, their approach to security was just abysmal, and it's hard to believe the rest of their operations are much better."

21. A former lead information analyst told reporters that Equifax shared unmasked social security numbers to company overseas. The employee said the company treated people's personally identifiable information as a "commodity."

22. Similarly, a former Equifax vice president of data quality reportedly wrote in a public post that "it bothered me how much access just about any employee had to the personally identifiable attributes. I would see printed credit files sitting near shredders, and I would hear people speaking about specific cases, speaking aloud consumer's personally identifiable information."

23. As a result of the Data Breach and its aftermath, Equifax Chairman and CEO Richard F. Smith stepped down. Equifax also fired its chief information

officer and chief security officer. The chief security officer, a college music major, had been criticized for lacking qualifications.

24. Congress and more than 30 states attorneys general are investigating the Data Breach. The Federal Trade Commission, in an unusual disclosure, said that it is also investigating the Data Breach.

25. Rather than spend adequate resources on data security, Equifax reportedly spent hundreds of thousands of dollars seeking to “reform” laws that impose liability on credit reporting agencies or require strict reporting of data breaches. In the months preceding the Data Breach, Equifax Inc. was lobbying lawmakers and federal agencies to ease up on regulation of credit-reporting companies. According to its congressional lobbying-disclosure reports, Equifax spent at least \$500,000 on lobbying Congress and federal regulators in the first half of 2017.

B. Equifax Failed to Release News of the Massive Breach Within a Timely Manner, and Its Response Has Been Deeply Flawed

26. Equifax reportedly discovered the Data Breach in July, but did not disclose the breach to the American public until September 7th. For months, consumers were unaware that some of their most valuable private information could be open, seen, and used by anybody. This personal information could include data about loans, loan payments and credit cards, as well as information on

everything from child support payments, credit limits, missed rent and utilities payments, addresses and employer history, which all factor into credit scores.

27. The impact of Equifax's delayed disclosure has been compounded by a botched response rollout, causing affected individuals additional harm and frustration. As computer security expert Brian Krebs wrote, "I cannot recall a previous data breach in which the breached company's public outreach and response has been so haphazard and ill-conceived as the one coming right now from big-three credit bureau Equifax."

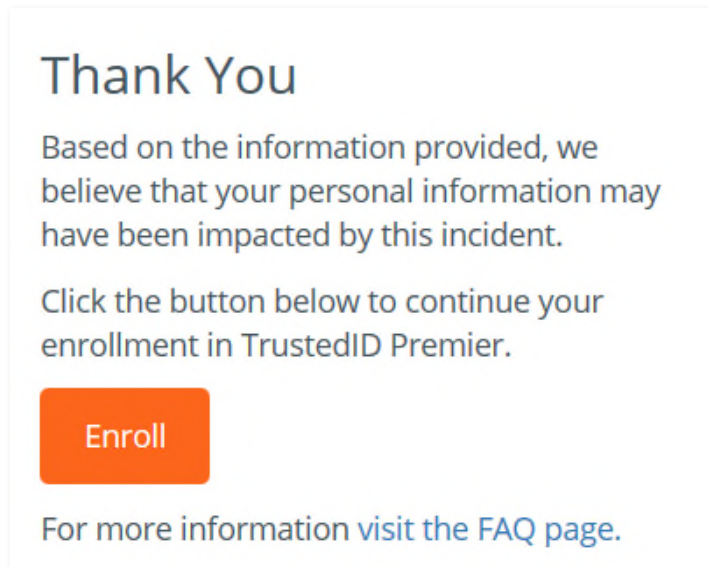
28. To begin with, the website that Equifax created to belatedly notify people of the Data Breach, www.equifaxsecurity2017.com, wrote Krebs, is "completely broken at best, and little more than a stalling tactic or sham at worst." For example, the website operates on a stock installation WordPress, which does not provide adequate security for website on which Equifax asks data breach victims to provide their last names and most of the Social Security number. As another indication of Equifax's slipshod approach, as reported by Ars Technica, Equifax left a username for administering the site in a page hosted on that site, "something that should never have happened":



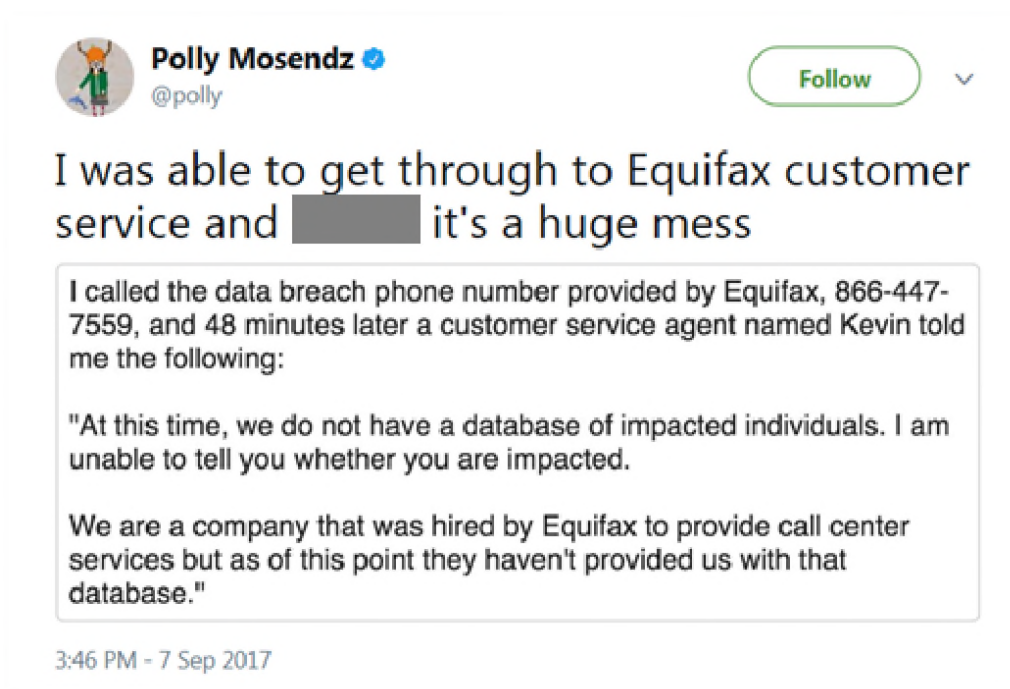
29. Those victims who were able to access the Equifax website to verify if they were victims of the Data Breach encountered more evidence of Equifax's bumbling response. To use the website, it appeared that Equifax was asking victims to give up any right to sue TrustedID, an Equifax entity providing identity monitoring services. Equifax appears to have changed the terms of service for that website after an outcry from consumers and consumer protection officials.

30. Aside from potentially luring victims into jeopardizing their right to sue, the Equifax website did not provide victims useful information on which they could act to protect their identities. Some victims who checked the website and were told they had not been affected were given the opposite answer when they checked later on a phone using the same information.

31. For example, entering two made-up identities—last names “Smith” and “Doe,” both with the last six Social Security number digits “123456”—yielded the same response:



32. Those victims who called the hotline set up to aid Equifax victims fared little better. They were greeted by unprepared customer service agents without any helpful information. This complaint provides one example:



33. Even now, weeks after the Data Breach, Equifax has not been able to provide Americans definitive answers about whether their most sensitive personal information has been exposed.

34. If a victim set up a credit freeze—one recommended, potentially expensive and time-consuming prophylactic—Equifax provided a 10-digit personal identification number (“PIN”). Such PINs are supposed to be difficult to guess, but the PINs Equifax is providing are based on the time and date the person set up a freeze; thus, undercutting one of the key tools victims can use to prevent identify theft.

35. In at least one instance, when a frustrated Equifax customer who had previously enrolled in Equifax’s paid monitoring service sought help online, Equifax directed them to a fake “phishing” website, securityequifax2017:



36. The website to which Equifax directed the consumer was critical of Equifax for using a domain name that could be so easily impersonated by phishing sites, leaving “millions vulnerable to phishing attacks on copycat sites”:



37. Similarly, in October visitors to Equifax’s website were confronted with fake download updates intended to trick them into installing malware on their computers. According to the website Arstechnica.com, “the net result is that the Equifax site was arguably compromised in some way, since administrators couldn’t control the pages visitors saw when trying to use key functions, some which

require visitors to enter Social Security numbers.” In response, Equifax took part of its website offline and blamed a vendor code running on Equifax’s website for “serving malicious content.”

C. Equifax’s Failures Have Harmed and Will Continue to Harm Breach Victims

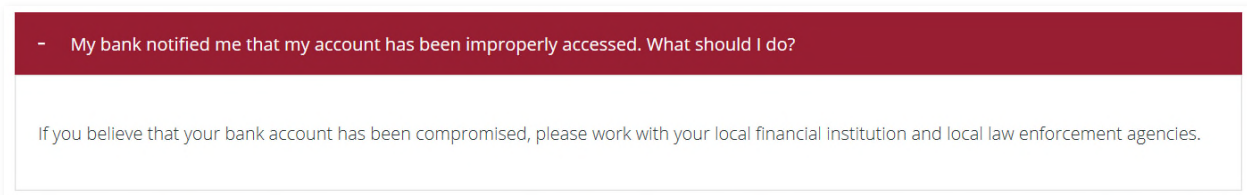
38. While Equifax’s response to the Data Breach has been almost comically inept, the harm for victims is terribly serious. As a result of the Data Breach, criminals now have access to the essential building blocks to steal the identities of 145.5 million Americans, roughly 44 percent of the population.

39. The Equifax Data Breach has greatly increased the victims’ risk of identity theft relative to the time before the Data Breach. Unlike the credit and debit card numbers stolen in some of the other recent high-profile data breaches, much of the information furnished here cannot simply be changed, and will continue to be valuable to identity thieves for many years.

40. As the Government Accountability Office reported in 2012, individuals who experience a data breach involving their Social Security number and dates of birth experience a much higher likelihood of being a victim of an identity crime. Social Security numbers, dates of birth, and names “are among the three personal identifiers most often sought by identity thieves,” according to the GAO.

41. The Equifax Data Breach released all those personal identifiers, putting victims at increased risk of credit/debit card fraud, financial identity theft, tax fraud/identity theft, account takeovers, social identity fraud, and other harms.

42. Equifax's website for providing information to Data Breach victims acknowledges that they may already have experienced identity theft, including an answer for people who have been notified by their bank that their account "has been improperly accessed":



43. The same website recommends that victims "remain vigilant for incidents of fraud and identity theft[.]"

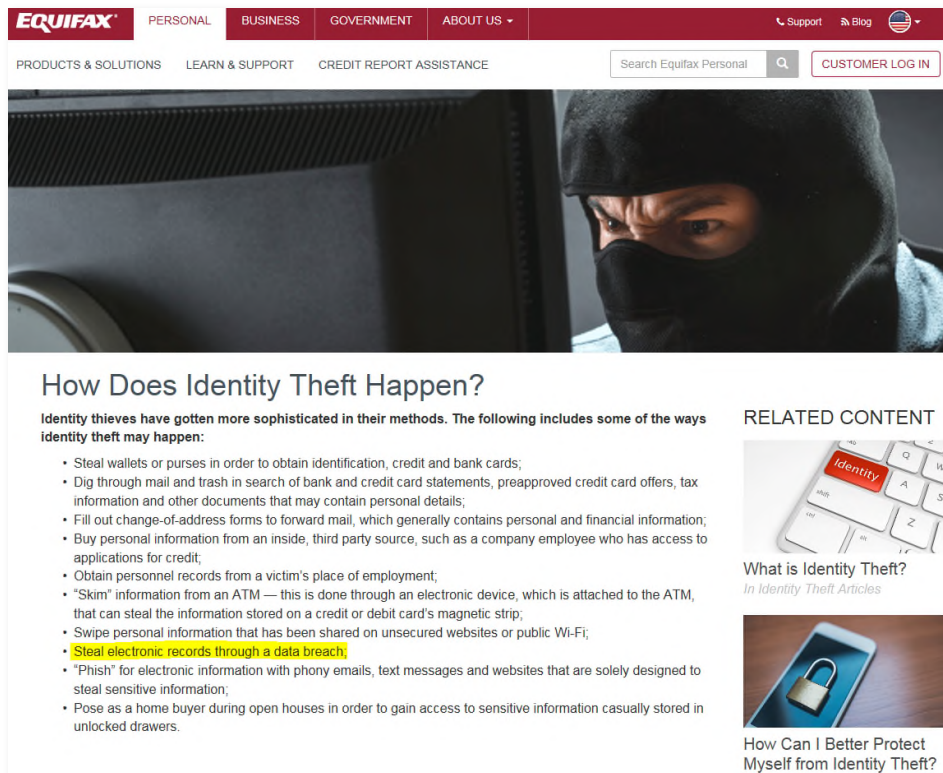
44. Equifax was aware of the increased risk of identity theft that data breaches cause, and the impacts of that identity theft. In fact, it appears that the hackers stole the credit card information, Social Security numbers, and addresses of over 200,000 individuals who had signed up for credit monitoring services through Equifax.

45. Equifax has published a pamphlet called "A Lasting Impact: The Emotional Toll of Identity Theft" discussing the "real" impacts that identity theft

victims face, which advises that to avoid identify theft people should keep their Social Security numbers, drivers licenses, and addresses private. (The data breach revealed about 10.9 million U.S. driver's licenses.)

46. Elsewhere, Equifax explained that to protect themselves from identify theft, people should “[k]eep your personal information secure online” and “[s]ecure your Social Security Number.”

47. One way identify theft could happen, Equifax warned, was the theft “of electronic records through a data breach”:



The screenshot shows the Equifax website's header with navigation links: PERSONAL, BUSINESS, GOVERNMENT, and ABOUT US. Below the header are links for PRODUCTS & SOLUTIONS, LEARN & SUPPORT, and CREDIT REPORT ASSISTANCE. A search bar and a CUSTOMER LOG IN button are also visible. The main content area features a large image of a person in a black balaclava looking at a computer screen. Below the image is the heading "How Does Identity Theft Happen?" followed by a paragraph stating that identity thieves have become more sophisticated. A bulleted list follows, detailing various methods of identity theft, including stealing wallets, digging through mail, filling out change-of-address forms, buying personal information from insiders, obtaining personnel records, skimming information from ATMs, swiping personal information from unsecured websites or public Wi-Fi, stealing electronic records through a data breach (highlighted in yellow), phishing for electronic information, and posing as a home buyer during open houses. To the right of the list is a "RELATED CONTENT" section with two articles: "What is Identity Theft?" and "How Can I Better Protect Myself from Identity Theft?", each accompanied by a small image.

EQUIFAX PERSONAL BUSINESS GOVERNMENT ABOUT US

Support Blog

PRODUCTS & SOLUTIONS LEARN & SUPPORT CREDIT REPORT ASSISTANCE

Search Equifax Personal

CUSTOMER LOG IN

How Does Identity Theft Happen?

Identity thieves have gotten more sophisticated in their methods. The following includes some of the ways identity theft may happen:

- Steal wallets or purses in order to obtain identification, credit and bank cards;
- Dig through mail and trash in search of bank and credit card statements, preapproved credit card offers, tax information and other documents that may contain personal details;
- Fill out change-of-address forms to forward mail, which generally contains personal and financial information;
- Buy personal information from an inside, third party source, such as a company employee who has access to applications for credit;
- Obtain personnel records from a victim's place of employment;
- "Skim" information from an ATM — this is done through an electronic device, which is attached to the ATM, that can steal the information stored on a credit or debit card's magnetic strip;
- Swipe personal information that has been shared on unsecured websites or public Wi-Fi;
- **Steal electronic records through a data breach;**
- "Phish" for electronic information with phony emails, text messages and websites that are solely designed to steal sensitive information;
- Pose as a home buyer during open houses in order to gain access to sensitive information casually stored in unlocked drawers.

RELATED CONTENT

What is Identity Theft?
In Identity Theft Articles

How Can I Better Protect Myself from Identity Theft?

48. Equifax has also acknowledged the increased risk that victims face by offering victims a one-year trial period of its proprietary credit monitoring service, TrustedID. But victims' increased risk of identity theft will last far beyond that one-year period. Identity thieves commonly wait years to commit fraud using breached data.

49. While victims are left vulnerable to identify theft, three top Equifax executives may have cashed out on the Data Breach, reportedly selling millions of dollars of stock after the company became aware of the breach but before the public found out.

V. CLASS ACTION ALLEGATIONS

A. Class Definition(s)

1. National Class

50. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seek relief on behalf of themselves and as representatives of a proposed nationwide class ("Nationwide Class"), defined as follows:

All natural persons in the United States whose personally identifying information ("PII") was compromised as a result of the Data Breach.

2. Statewide Classes

51. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert claims under the laws of individual states, and on behalf of separate statewide subclasses, for each of the following states:

- a. Washington
- b. Connecticut
- c. Maryland
- d. North Carolina
- e. Nebraska
- f. Pennsylvania

Each proposed statewide class (“Statewide Class”) is defined as follows:

All natural persons who are citizens of [STATE] whose PII was compromised as a result of the Data Breach.

52. Except where otherwise noted, “Class” or “Class members” shall refer to members of the Nationwide Class and each of the Statewide Classes.

53. Excluded from the Class are Defendant and any of its affiliates, parents or subsidiaries; all employees of Defendant; as well as the Court and its personnel presiding over this action.

54. **Numerosity.** The proposed Class is sufficiently numerous, as over 145 million Data Breach victims had their PII compromised, and they are dispersed

throughout the United States, making joinder of all members impracticable. Class members can be readily identified and ascertained through the records maintained by Equifax.

55. **Commonality.** Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual class members, including:

- a. Whether Equifax had a legal duty to use reasonable security measures to protect Class members' PII;
- b. Whether Equifax timely, accurately, and adequately informed Class members that their PII had been compromised;
- c. Whether Equifax breached its legal duty by failing to protect Class members' PII;
- d. Whether Equifax acted reasonably in securing Class members' PII;
- e. Whether Class members are entitled to actual damages and/or statutory damages; and
- f. Whether Class members are entitled to injunctive relief.

56. **Typicality.** Plaintiffs' claims are typical of the claims of members of the proposed Class because, among other things, Plaintiffs and Class members sustained similar injuries as a result of Equifax's uniform wrongful conduct and their legal claims all arise from the same conduct by Equifax.

57. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the proposed Class. Plaintiffs' interests do not conflict with other Class

members' interests and they have retained counsel experienced in complex class action and data privacy litigation to prosecute this case on behalf of the Class.

58. **Rule 23(b)(3).** In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual Class members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing Equifax's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

59. **Rule 23(b)(2).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). Equifax has acted or refused to act on grounds that apply generally to the proposed Class, making final declaratory or injunctive relief appropriate with respect to the proposed Class as a whole.

60. **Rule 23(c)(4).** This action also satisfies the requirements for maintaining a class action under Rule 23(c)(4). The claims of Class members are composed of particular issues that are common to all Class members and capable of class wide resolution that will significantly advance the litigation.

VI. CLAIMS FOR RELIEF

Claims Asserted on Behalf of the Nationwide Class:

COUNT I — WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT, 15 U.S.C. §§ 1681 ET SEQ.

1. Overview

61. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

62. Plaintiffs and the Class bring this claim to recover damages suffered as a result of Equifax's below-described willful violations of the Fair Credit Reporting Act (herein, "FCRA" or "the Act"), 15 U.S.C. §§ 1681 et seq.

63. As individuals, Plaintiffs and Nationwide Class members are consumers entitled to the protections of FCRA. 15 U.S.C. § 1681a(c).

64. Congress, in enacting FCRA, found that "[c]onsumer reporting agencies," like Equifax, "have assumed a vital role in assembling and evaluating consumer credit and other information on consumers" and, as a result, "[t]here is a

need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy." 15 U.S.C. § 1681(a)(3)-(4) (emphasis added).

65. Under FCRA, a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties" 15 U.S.C. § 1681a(f).

66. Equifax is a consumer reporting agency under FCRA because it, for monetary fees, regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

67. Congress further noted that one purpose of the Act is to "require 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." *See* 15 U.S.C. § 1681(b) (emphasis added).

68. As detailed below, Equifax failed to fulfill its statutory obligations under the Act by, at a minimum: (a) failing to adopt reasonable procedures to protect the confidentiality, privacy, and proper utilization of Plaintiffs' and the Nationwide Class members' personal consumer, credit, and other personally-identifying information including names, social security numbers, credit card numbers, account numbers, credit histories and other credit data; (b) furnishing and/or disclosing that information to improper third parties; (c) failing to take swift action upon learning of unauthorized access to Plaintiffs' and the Nationwide Class members' personal information and its unauthorized dissemination to third parties; and (d) disclosing, exposing, and/or making known to unauthorized third parties, the medical information of Plaintiffs and Nationwide Class members.

2. Violations of 15 U.S.C. § 1681e(a) – Willful Failure to Maintain Reasonable Security Measures

69. 15 U.S.C. § 1681e(a) requires that “consumer reporting agenc[ies],” such as Equifax, “shall maintain reasonable procedures designed to avoid violations of section 1681c of this title and to limit the furnishing of consumer reports to the purposes listed under [15 U.S.C. § 1681b].” 15 U.S.C. § 1681e(a).

70. These procedures, the Act goes on to explain: “shall require that prospective users of the information identify themselves, certify the purposes for

which the information is sought, and certify that the information will be used for no other purpose.” *Id.*

71. Moreover, the Act directs that “[n]o consumer reporting agency may furnish a consumer report to any person if it has reasonable grounds for believing that the consumer report will not be used for a [permissible] purposed listed in section 1681b of this title.” *Id.*

72. The Federal Trade Commission has explained that 15 U.S.C. § 1681e(a) requires consumer reporting agencies to “have reasonable and effective procedures to limit unauthorized access to its databases. Such procedures may include a system of monitoring access to its database of consumer reports, including a system to monitor anomalies and other suspicious activity to guard against unauthorized access Procedures also may include . . . installation and use of appropriate computer hardware and software. . . .” Fed. Trade Comm’n, 40 Years of Experience with the Fair Credit Reporting Act at 66 (July 2011).

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

74. Equifax violated Section 1681e(a) by failing to implement and maintain reasonable, industry-standard security measures to ensure that Plaintiffs' and the Nationwide Class members' consumer credit information was not accessed for an impermissible purpose.

75. Equifax further violated Section 1681e(a) by failing to require prospective users of information to identify themselves as well as their purpose before permitting them access to Plaintiffs' and the Nationwide Class members' consumer credit information.

76. Equifax's failure to adopt and maintain such protective procedures directly and proximately resulted in the theft of and improper access to Plaintiffs' and the Nationwide Class members' consumer and credit information as well as its wrongful dissemination to unauthorized third parties in the public domain.

3. Violations of 15 U.S.C. § 1681b(a) – Furnishing Consumer Data Without a Permissible Purpose

77. 15 U.S.C. § 1681b provides that a “consumer reporting agency,” like Equifax, “may furnish a consumer report under the following circumstances and no other:” (1) in response to a court order; (2) in response to a consumer request; (3) to a person which it has reason to believe will use the information for a credit, employment, insurance, licensing, or other legitimate business purpose; and (4) in response to a request by a government agency. *Id.*

78. FCRA defines a “consumer report” as: “[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer’s eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b).” 15 U.S.C. § 1681a(d)(1).

79. Plaintiffs’ and the Nationwide Class members’ personally-identifying and other consumer information including their names, social security numbers, credit card numbers, account numbers, credit history, and other credit data constitute a “consumer report” within the meaning of 15 U.S.C. § 1681a(d)(1) because that information bears on their credit-worthiness, personal characteristics, and character and was collected by Equifax for the purpose of establishing their eligibility for credit.

80. Equifax violated § 1681b by furnishing and/or providing a written, oral, or other communications and/or documents and files which contained Plaintiffs’ and the Nationwide Class members’ personally-identifying and other

consumer information to unauthorized third parties, who Equifax had no reason to believe would use the information for a permissible purpose.

4. Violations of 15 U.S.C. § 1681b(g) – Willful Disclosure of Confidential Medical Data

81. In addition to ensuring the protection of personal consumer credit data, FCRA lays out special requirements for consumer reporting agencies with respect to confidential medical information, and restricting its dissemination or disclosure. *See, e.g.*, 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681 c(a)(6).

82. Upon information and belief Equifax maintains “medical information” as a component of its effort to assess the credit-worthiness of consumers. Indeed, according to a review published by the Federal Reserve, nearly half of debt collection tradelines on credit reports are for medical debts. *See* Robert Avery, Paul Calem, Glenn Canner, & Raphael Bostic, An Overview of Consumer Data and Credit Reporting, Fed. Reserve Bulletin (RB), p. 69 (Feb. 2003).

83. Equifax violated § 1681b by disclosing, exposing, and/or making known to unauthorized third parties, the medical information of Plaintiffs and the Nationwide Class members, as detailed herein, and they were harmed as a result.

5. Violations of 15 U.S.C. § 1681c-1 – Willful Failure to Respond to Suspected Identify Theft

84. 15 U.S.C. § 1681c-1 imposes obligations on consumer reporting agencies like Equifax upon suspicion of fraud or identity theft.

85. Specifically, § 1681c-1 provides that “[u]pon the direct request of a consumer, or an individual acting on behalf of . . . of a consumer, who asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft, a consumer reporting agency shall . . . include a fraud alert in the file of that consumer . . . for a period of not less than 90 days . . . and refer the information regarding the fraud alert . . . to each of the other consumer reporting agencies,” and provide certain disclosures to consumers as noted in §1681c-1(a)(2). *See* 15 U.S.C. § 1681c-1(a)(2).

86. On information and belief, Equifax was given notice of that fact that millions of consumers were at risk of becoming the victim of fraud and identity theft due to the unprecedented Data Breach described above, more than one month before it was made known to the public.

87. Nevertheless, and in violation of its obligations under 15 U.S.C. § 1681c-1, Equifax did not make timely disclosures to affected consumers, did not include fraud alerts to prevent identity theft following the Data Breach, and did not make timely notifications to other consumer reporting agencies; as a result, in

addition to the harm described herein, Plaintiffs and the Nationwide Class were put at additional risk of fraud and identity theft, and were forced to incur additional costs to prevent the theft themselves.

6. Plaintiffs and the Nationwide Class Suffered Damages as a Proximate Result of Equifax's Willful Violations of FCRA and are Entitled to Relief

88. Equifax willfully violated the above-described provision of FCRA. The willful nature of Equifax's violations is supported by Equifax's other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

89. Equifax also acted willfully because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised it of its duties under the FCRA. Any reasonable consumer reporting agency knows or should

know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other members of the classes of their rights under the FCRA.

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

91. As a direct and proximate result of Equifax's willful violations of FCRA, and the resulting Data Breach described above, the personally-identifying and consumer credit information of Plaintiffs and the Nationwide Class members was stolen and made accessible to unauthorized third parties in the public domain.

92. As a direct and proximate result of Equifax's willful violations of FCRA, and the resulting Data Breach described above, Plaintiffs and Nationwide Class members were and continue to be damaged in the form of, without limitation, an increased cost of credit associated with misuse of their credit data, expenses for credit monitoring and identity theft insurance, other out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

93. As a result of Equifax's willful failure to "to comply with any requirement imposed under" the Act, it is liable to Plaintiffs and the Nationwide Class members for actual and statutory damages, together with their fees and costs. *See* 15 U.S.C. § 1681n (discussing willful noncompliance).

94. Plaintiffs and the Nationwide Class members, therefore, are entitled to compensation for their actual damages including, *inter alia*, (i) an increased cost of credit associated with misuse of their credit data; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach described above; (iii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iv) deprivation of the value of their personally-identifying information,, and credit data for which there is a well-established national and international market; (v) anxiety and emotional distress; together with (vi) statutory damages of not less than \$100, and not more than \$1000, each; and (vii) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. § 1681n(a).

**COUNT II —
Negligent Violation of the Fair Credit Reporting Act**

95. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

96. Plaintiffs and the Nationwide Class bring this claim to recover damages suffered as a result of Equifax's below-described negligent violations of the Fair Credit Reporting Act (herein, "FCRA" or "the Act"), 15 U.S.C. §§ 1681 et seq.

97. As detailed above, as individuals, Plaintiffs and Nationwide Class members are consumers entitled to the protections of FCRA, 15 U.S.C. § 1681a(c), and 15 U.S.C. § 1681a(f).

98. Equifax is a consumer reporting agency under FCRA because it, for monetary fees, regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties. 15 U.S.C. § 1681 a(f).

99. As detailed above, Equifax failed to fulfill its statutory obligations under the Act by, at a minimum: (a) failing to adopt reasonable procedures to protect the confidentiality, privacy, and proper utilization of Plaintiffs and the Nationwide Class members' personal consumer, credit, and other personally-identifying information including their names, social security numbers, credit card numbers, account numbers, credit histories and other credit data; (b) furnishing and/or disclosing that information to improper third parties; (c) failing to take swift action upon learning of unauthorized access to Plaintiffs and the Nationwide Class

members' personal information and its unauthorized dissemination to third parties; and (d) disclosing, exposing, and/or making known to unauthorized third parties, the medical information of Plaintiffs and Nationwide Class members.

100. Specifically, Equifax violated FCRA by willfully and/or negligently (1) failing to adopt and maintain reasonable procedures to protect the confidentiality of consumer information in violation of 15 U.S.C. § 1681e; (2) furnishing and/or disclosing consumer information to unauthorized third parties without a permissible purpose in violation of 15 U.S.C. § 1681b; (3) disclosing confidential medical information in violation of 15 U.S.C. §§ 1681b(g)(4), and 1681b(g)(3)(A); and (4) failing to respond to identity theft or the suspicion of identity theft in violation of 15 U.S.C. § 1681c-1.

101. 15 U.S.C. § 1681b provides that a "consumer reporting agency," like Equifax, "may furnish a consumer report under the following circumstances and no other:" (1) in response to a court order; (2) in response to a consumer request; (3) to a person which it has reason to believe will use the information for a credit, employment, insurance, licensing, or other legitimate business purpose; and (4) in response to a request by a government agency. *Id.*

102. FCRA defines a "consumer report" as: "[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a

consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b)." 15 U.S.C. § 1681a(d)(1).

103. Plaintiffs and the Nationwide Class members' personally-identifying and other consumer information including their names, social security numbers, credit card numbers, account numbers, credit history, and other credit data constitute a "consumer report" within the meaning of 15 U.S.C. § 1681a(d)(1) because that information bears on their credit-worthiness, personal characteristics, and character and was collected by Equifax for the purpose of establishing their eligibility for credit.

104. Equifax violated § 1681b by furnishing and/or providing a written, oral, or other communications and/or documents and files which contained Plaintiffs and the Nationwide Class members' personally-identifying and other consumer information to unauthorized third parties, who Equifax had no reason to believe would use the information for a permissible purpose.

105. Equifax negligently violated the above-described provision of FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by Equifax's other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

106. Equifax's negligent conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Nationwide Class members' personal information for no permissible purposes under FCRA.

107. As a direct and proximate result of Equifax's negligent violations of FCRA, and the resulting Data Breach described above, the personally-identifying and consumer credit information of Plaintiffs and the Nationwide Class members was stolen and made accessible to unauthorized third parties in the public domain.

108. As a direct and proximate result of Equifax's negligent violations of FCRA, and the resulting Data Breach described above, Plaintiffs and Nationwide Class members were and continue to be damaged in the form of, without limitation, an increased cost of credit associated with misuse of their credit data, expenses for credit monitoring and identity theft insurance, other out-of-pocket

expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

109. Plaintiffs and Nationwide Class members, therefore, are entitled to compensation for their actual damages including, inter alia, (i) an increased cost of credit associated with misuse of their credit data; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Data Breach described above; (iii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iv) deprivation of the value of their personally-identifying information,, and credit data for which there is a well-established national and international market; (v) anxiety and emotional distress; together with (vi) attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. § 1681o(a).

**COUNT III —
Negligence**

110. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

111. Equifax owed a duty to Plaintiffs and the Nationwide Class members to exercise reasonable care in safeguarding and protecting their highly sensitive and personal information. This duty included, among other things, designing,

maintaining, monitoring, testing Equifax's security systems, protocols, and practices, as well as taking other reasonable security measures to protect and adequately secure the PII of Plaintiffs and Nationwide Class members from unauthorized access.

112. Equifax owed a duty to Class members to implement administrative, physical and technical safeguards, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiffs' and Nationwide Class members' PII.

113. Equifax owed a duty of care to Plaintiffs and Nationwide Class members because they were foreseeable and probable victims of any inadequate security practices. It was foreseeable that if Equifax did not take reasonable security measures, the PII of Plaintiffs and members of the Nationwide Class would be stolen. Major corporations, and particularly credit rating agencies, like Equifax face a higher threat of security breaches than smaller companies due in part to the large amounts of data they possess. Equifax knew or should have known its security systems were inadequate, particularly in light of the prior data breaches that Equifax had experienced, and yet Equifax failed to take reasonable precautions to safeguard the PII of Plaintiffs and members of the Nationwide Class.

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

115. Equifax had a duty to timely and accurately notify Plaintiffs and Nationwide Class members if their PII was compromised so that Plaintiffs and Nationwide Class members could act to mitigate the harm caused by the loss of opportunity to control how their PII was used.

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

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

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

119. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PII and consumer reports for no permissible purposes under FCRA.

120. As a result of Equifax's willful failure to prevent the Data Breach, Plaintiffs and Nationwide Class members suffered injury, which includes but is not limited to: (1) exposure to a heightened, imminent risk of fraud, identity theft, and financial harm; (2) the loss of the opportunity to control how their PII is used; (3) the diminution in the value and/or use of their PII; (4) the compromise, publication, and/or theft of their PII; (5) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial accounts; (6) lost opportunity costs associated with the effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft, as well as the time and effort Plaintiffs and Nationwide Class members have expended to monitor their financial accounts and credit histories to guard against identity theft; (7) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (8) unauthorized use of compromised PII to

open new financial accounts; (9) tax fraud and/or other unauthorized charges to financial accounts and associated lack of access to funds while proper information is confirmed and corrected; (10) the continued risk to their PII, which remain in Equifax's possession and are subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives.

121. The damages to Plaintiffs and Nationwide Class members were a proximate, reasonably foreseeable result of Equifax's breaches of its duties.

122. Plaintiffs and the Nationwide Class are also entitled to damages and reasonable attorneys' fees and costs. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

**COUNT IV —
Negligence Per Se**

123. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

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

125. Under FCRA, 15 U.S.C. § 168b, a “consumer reporting agency,” like Equifax, “may furnish a consumer report under the following circumstances and no other:” (1) in response to a court order; (2) in response to a consumer request; (3) to a person which it has reason to believe will use the information for a credit, employment, insurance, licensing, or other legitimate business purpose; and (4) in response to a request by a government agency. *Id.*

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

127. Under 15 U.S.C. § 1681c-1, FCRA imposes obligations on consumer reporting agencies like Equifax to make timely disclosures to consumers upon suspicion of fraud or identity theft.

128. Specifically, § 1681c-1 provides that “[u]pon the direct request of a consumer, or an individual acting on behalf of . . . of a consumer, who asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft, a consumer reporting agency shall .

. . . include a fraud alert in the file of that consumer . . . for a period of not less than 90 days . . . and refer the information regarding the fraud alert . . . to each of the other consumer reporting agencies,” and provide certain disclosures to consumers as noted in § 1681c-1(a)(2). *See* 15 U.S.C. § 1681c-1(a)(2).

129. On information and belief, Equifax was given notice of the fact that millions of consumers were at risk of becoming the victim of fraud and identity theft due to the unprecedented Data Breach described above, months before it was made known to the public.

130. Nevertheless, and in violation of its obligations under 15 U.S.C. § 1681c-1, Equifax did not make timely disclosures to affected consumers, did not include fraud alerts to prevent identity theft following the Data Breach, and did not make timely notifications to other consumer reporting agencies; as a result, in addition to the harm described herein, Plaintiffs and the Nationwide Class were put at additional risk of fraud and identity theft, and were forced to incur additional costs to prevent the theft themselves.

131. Under 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681 c(a)(6), FCRA imposes requirements for consumer reporting agencies with respect to confidential medical information, and restricting its dissemination or disclosure. In violation of these obligations, Equifax disclosed, exposed, and/or made known to unauthorized

third parties, the medical information of Plaintiffs and the Nationwide Class members.

132. Plaintiffs and the Nationwide Class members are within the class of persons that FCRA was intended to protect.

133. Plaintiffs and Nationwide Class members were foreseeable victims of Equifax's violation of FCRA. Equifax knew or should have known that a breach of its data security systems would cause injuries to Nationwide Class members.

134. Equifax likewise violated Section 5(a) of the FTC Act, which provides that 'unfair or deceptive acts or practices in or affecting commerce...are...declared unlawful.' 15 U.S.C. § 45(a)(1).

135. By failing to use reasonable measures to protect consumers' PII and by not complying with applicable industry standards as discussed above, Equifax violated Section 5 of the FTC Act. Equifax's conduct was particularly unreasonable given the sensitive nature and vast amount of PII it had collected, obtained and stored, and the foreseeable consequences that a data breach of this information would substantially harm Plaintiffs and the Nationwide Class.

136. Equifax was required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards:

- (1) to insure the security and confidentiality of customer records and information;
- (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
- (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

137. In order to satisfy its obligations under the GLBA, Equifax was also required to “develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue.” *See* 16 C.F.R. § 314.4

138. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to “develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems.” *See id.*

139. Further, when Equifax became aware of “unauthorized access to sensitive customer information,” it should have “conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or

will be misused” and “notif[ied] the affected customer[s] as soon as possible.” *See id.*

140. Equifax violated the GLBA by failing to “develop, implement, and maintain a comprehensive information security program” with “administrative, technical, and physical safeguards” that were “appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue.” This includes, but is not limited to, Equifax’s failure to implement and maintain adequate data security practices to safeguard Nationwide Class members’ PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendant’s data security practices were inadequate to safeguard Nationwide Class members’ PII.

141. Equifax also violated the GLBA by failing to “develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems.” This includes, but is not limited to, Equifax’s failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

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

143. Plaintiffs and Nationwide Class members were foreseeable victims of Equifax's violation of the GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately notify the appropriate regulatory authorities, law enforcement, and Nationwide Class members themselves would cause damages to Nationwide Class members.

144. Defendant's failure to comply with the applicable laws and regulations, including FCRA, the FTC Act and the GLBA, constitutes negligence per se.

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

146. As a direct and proximate result of Equifax's negligence per se, Plaintiffs and the Nationwide Class members suffered, and continue to suffer, injuries, which include but are not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Nationwide Class

members must more closely monitor their financial accounts and credit histories to guard against identity theft. Nationwide Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs and Nationwide Class members' PII has also diminished the value of their PII.

147. Therefore, Plaintiffs and Nationwide Class members are entitled to damages in an amount to be proven at trial.

**COUNT V —
Declaratory Judgment**

148. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

149. As previously alleged, Plaintiffs and the Nationwide Class have stated claims against Equifax based on negligence and statutory violations.

150. Equifax has failed to live up to its obligations to provide reasonable security measures for the PII of Plaintiffs and the Nationwide Class.

151. Equifax still possesses PII pertaining to Plaintiffs and Nationwide Class members.

152. In addition, the Data Breach has rendered Equifax's system even more vulnerable to unauthorized access and requires that Equifax immediately take even

more stringent measures to currently safeguard the PII of Plaintiffs and the Nationwide Class going forward.

153. Equifax has made no representation that it has remedied the vulnerabilities in its data security systems.

154. An actual controversy has arisen in the wake of the Data Breach regarding Equifax's current obligations to provide reasonable data security measures to protect the PII of Plaintiffs and the Nationwide Class. On information and belief, Equifax maintains that its security measures were, and remain, reasonably adequate. On information and belief, Equifax further denies that it previously had or now has any obligation to better safeguard the PII of Plaintiffs and the Nationwide Class.

155. Plaintiffs thus seek a declaration that to comply with its existing obligations, Equifax must implement specific additional, prudent industry security practices, as outlined below, to provide reasonable protection and security to the PII of Plaintiffs and the Nationwide Class.

156. Specifically, Plaintiffs and the class seek a declaration that (a) Equifax's existing security measures do not comply with its obligations, and (b) that to comply with its obligations, Equifax must implement and maintain reasonable security measures on behalf of Plaintiffs and the Nationwide Class,

including, but not limited to: (1) engaging third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis; (2) engaging third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) auditing, testing, and training its security personnel regarding any new or modified procedures; (4) purging, deleting and destroying, in a secure manner, data not necessary for its business operations; (5) conducting regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receiving periodic compliance audits by a third party regarding the security of the computer systems Equifax uses to store the personal information of Plaintiffs and the Nationwide Class members; (8) meaningfully educating Plaintiffs and the Nationwide Class members about the threats they face as a result of the loss of their PII to unauthorized third parties, as well as the steps they must take to protect themselves; and (9) providing ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and Nationwide Class members.

Claims Asserted on Behalf of Statewide Classes

Claims Asserted on Behalf of the Washington Statewide Class

**COUNT VI —
Violation of the Washington Data Breach Notice Act, Wash. Rev. Code.
§§ 19.255.10, *et seq.***

157. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

158. Plaintiff Dori Mashburn brings this cause of action on behalf of the Washington Statewide Class.

159. Under Wash. Rev. Code Ann. § 19.255.010(1), “[a]ny person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person”

160. Under Wash. Rev. Code Ann. § 19.255.010(2), “[a]ny person or business that maintains 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.”

161. Under Wash. Rev. Code Ann. § 19.255.010 (16), “[n]otification to affected consumers ... under this section must be made in the most expedient time possible and without unreasonable delay, no more than forty-five calendar days after the breach was discovered.”

162. Equifax conducts business in Washington and owns or licenses computerized data that includes personal information, as defined by Wash. Rev. Code Ann. § 19.255.010.

163. Plaintiff and the Washington Statewide Class members’ PII (including but not limited to names, addresses, and social security numbers) includes personal information covered under Wash. Rev. Code Ann. § 19.255.010(5).

164. Because Equifax discovered a breach of its security system in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured, Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under Wash. Rev. Code Ann. § 19.255.010(16).

165. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated Wash. Rev. Code Ann. § 19.255.010(16).

166. As a direct and proximate result of Equifax's violations of Wash. Rev. Code Ann. § 19.255.010(16), Plaintiff and the Washington Statewide Class members suffered the damages described above.

167. Plaintiff and the Washington Statewide Class members seek relief under Wash. Rev. Code Ann. §§ 19.255.010(13)(a), (b) including but not limited to actual damages (to be proven at trial) and injunctive relief.

**COUNT VII —
Violation of Washington Consumer Protection Act, Wash. Rev. Code
§§ 19.86.020, *et seq.***

168. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

169. Plaintiff Dori Mashburn brings this cause of action on behalf of the Washington Statewide Class.

170. Equifax, while operating in Washington, engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Wash. Rev. Code § 19.86.020. This includes but is not limited to the following:

- Equifax failed to enact adequate privacy and security measures to protect the Washington Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;
- Equifax failed to take proper action following known security risks, which was a direct and proximate cause of the Data Breach;

- Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Washington Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft;
- Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for the Washington Statewide Class members' PII;
- Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Washington Statewide Class members' PII, including but not limited to duties imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. §§ 6801 et seq.;
- Equifax failed to maintain the privacy and security of the Washington Statewide Class members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach; and
- Equifax failed to disclose the Data Breach to the Washington Statewide Class members in a timely and accurate manner, in violation of the duties imposed by Wash. Rev. Code Ann. § 19.255.010(1).

171. As a direct and proximate result of Equifax's practices, the Washington Statewide Class members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

172. The above unfair and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Washington Statewide Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

173. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the Washington Statewide Class members' PII and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-described unfair practices and deceptive acts were negligent, knowing and willful.

174. Plaintiff and the Washington Statewide Class members seek relief pursuant to Wash. Rev. Code § 19.86.090, including but not limited to actual damages (to be proven at trial), treble damages, injunctive relief, and attorneys' fees and costs.

Claims Asserted on Behalf of the Connecticut Statewide Class

**COUNT VIII —
Violation of the Connecticut Unfair Trade Practices Act, Conn. Gen.
Stat. § 42-110, *et seq.***

175. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

176. Plaintiff Sarah L. Hardy brings this cause of action on behalf of the Connecticut Statewide Class.

177. Equifax and the Connecticut Statewide Class members are “persons” within the meaning of Conn. Gen. Stat. § 42-110a(3) of the Connecticut Unfair Trade Practices Act (“Connecticut UTPA”). Equifax is engaged in “trade” or “commerce” within the meaning of Conn. Gen. Stat. § 42-110a(4).

178. The Connecticut UTPA provides: “No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.” Conn. Gen. Stat. § 42-110b(a).

179. In the course of its business, Defendant Equifax, through its agents, employees, and/or subsidiaries, violated the Connecticut UTPA as detailed above. Specifically, failing to adequately protect the sensitive information of Connecticut Statewide Class members and failing to adequately respond to a data breach, Defendant engaged in one or more of the following unfair or deceptive acts or practices in violation of Conn. Gen. Stat. § 42-110b(a):

- Causing likelihood of confusion or of misunderstanding as to security of Connecticut Statewide Class members sensitive information;
- Representing that the Equifax’s information security systems and practices have characteristics or benefits that they do not have;
- Engaging in other conduct which created a likelihood of confusion or of misunderstanding; and/or

- Using or employing deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of a material fact with intent that others rely upon such concealment, suppression or omission, in connection with the advertisement and sale of Equifax's goods or services, whether or not any person has in fact been misled, deceived or damaged thereby.

180. Defendant's scheme and concealment of the true characteristics of its information security systems were material to Plaintiff and the Connecticut Statewide Class, as Defendant intended. Had they known the truth, Plaintiff and the Connecticut Statewide Class would not have permitted Equifax to retain their sensitive information.

181. Plaintiff and Connecticut Statewide Class members had no way of discerning that Defendant's representations were false and misleading, or otherwise learning the facts that Defendant had concealed or failed to disclose, because Defendant did not disclose the true nature of its information security systems and practices.

182. Defendant had an ongoing duty to Plaintiff and the Connecticut Statewide Class to refrain from unfair and deceptive practices under the Connecticut UTPA in the course of its business. Specifically, Defendant owed Plaintiff and Connecticut Statewide Class members a duty to disclose all the material facts concerning its information security systems and practices because it possessed exclusive knowledge, they intentionally concealed it from Plaintiff and

the Connecticut Statewide Class, and/or they made misrepresentations that were rendered misleading because they were contradicted by withheld facts.

183. Plaintiff and Connecticut Statewide Class members suffered ascertainable loss and actual damages as a direct and proximate result of Defendant's concealment, misrepresentations, and/or failure to disclose material information.

184. Defendant's violations present a continuing risk to Plaintiff and the Connecticut Statewide Class, as well as to the general public. Defendant's unlawful acts and practices complained of herein affect the public interest.

185. Pursuant to Conn. Gen. Stat. § 42-110g, Plaintiff and the Connecticut Statewide Class seek an order enjoining Defendant's unfair and/or deceptive acts or practices, and awarding damages, punitive damages, and any other just and proper relief available under the Connecticut UTPA.

Claims Asserted on Behalf of the Maryland Statewide Class

COUNT IX —

Violation of the Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), and (iv) and (9)(i), *et seq.*

186. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

187. Plaintiffs Richard Gainey and Valerie Gainey bring this cause of action on behalf of the Maryland Statewide Class.

188. Maryland Statewide Class members are “consumers” as meant by Md. Code Ann., Com. Law § 13-101.

189. Equifax provides “consumer goods” and/or “consumer services” as meant by Md. Code Ann., Com. Law § 13-101.

190. The unlawful trade practices, misrepresentations, and omissions described herein did not constitute “professional services” on the part of Defendant.

191. Defendant Equifax, while operating in Maryland, engaged in unlawful trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services in violation of Md. Code Ann., Com. Law § 13-301, including but not limited to the following:

- Equifax misrepresented material facts to the Maryland Statewide Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Maryland Statewide Class members’ Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of Md. Code Ann., Com. Law § 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);
- Equifax misrepresented material facts to the Maryland Statewide Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of

Maryland members' Personal Information in violation of Md. Code Ann., Com. Law § 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);

- Equifax omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Maryland Statewide Class members' Personal Information in violation of Md. Code Ann., Com. Law § 13-301(1), (2)(i), (2)(iv), (3), (5)(i), (9)(i), (9)(iii), and 14(xxi);
- Equifax engaged in unfair acts and practices by failing to maintain the privacy and security of Maryland Statewide Class members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d et. seq.), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Maryland's Confidentiality of Medical Records Act (Md. Code Ann., Health-Gen. §§ 4-302; 4-303(a)); Maryland's Disclosure Requirements for Insurers statute (Md. Code, Ins. § 4-403); Maryland's Disclosure Requirements for Nonprofit Health Service Plans statute (Md. Code, Ins. § 14-138); Maryland's Privacy of Consumer Financial and Health Information regulations (Md. Code Regs. 31.16.08.01, et seq.); Maryland's data breach statute (Md. Code Ann. Com. Law § 14-3503), and Maryland's Social Security Number Privacy Act (Md. Code Ann., Com. Law § 14-3401, et seq.);
- Equifax engaged in unfair acts and practices by failing to disclose the Data Breach to Maryland Statewide Class members in a timely and accurate manner, in violation of Md. Code Com. Law § 14-3504(b)(3);
- Equifax engaged in unfair acts and practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Maryland Statewide Class members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

192. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial

injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

193. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard Maryland Statewide Class members' Personal Information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Maryland Statewide Class.

194. As a direct and proximate result of Defendant's unlawful practices, Maryland Statewide Class members suffered injury and/or damages.

195. Maryland Statewide Class members seek relief under Md. Code Ann., Com. Law § 13-408, including, but not limited to, damages, injunctive relief, and attorneys' fees and costs.

Claims Asserted on Behalf of the North Carolina Statewide Class

COUNT X — Violation of the North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), et seq.;

196. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

197. Plaintiffs Jonathan and Carrie Entsminger bring this cause of action on behalf of the North Carolina Statewide Class.

198. Equifax, while operating in North Carolina, engaged in unfair or deceptive acts and practices affecting commerce, in violation of N.C. Gen. Stat. § 75-1.1. This includes but is not limited to the following:

- Equifax failed to enact adequate privacy and security measures to protect North Carolina Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;
- Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Equifax knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the North Carolina Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft;
- Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for North Carolina Statewide Class members' PII;
- Equifax knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of North Carolina Statewide Class members' PII, including but not limited to duties imposed by the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801 et seq., and the North Carolina Consumer and Customer Information Privacy Act, N.C. Gen. Stat. § 58-39-1, et seq.;
- Equifax failed to maintain the privacy and security of North Carolina Statewide Class members' PII, in violation of duties imposed by applicable

federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach; and

- Equifax failed to disclose the Data Breach to North Carolina Statewide Class members in a timely and accurate manner, in violation of duties imposed by N.C. Gen. Stat. Ann. § 75-65.

199. As a direct and proximate result of Equifax's practices, North Carolina Statewide Class members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

200. The above unfair and deceptive acts and practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to North Carolina Statewide Class members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

201. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard North Carolina Statewide Class members' PII and that risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing, willful, and/or wanton and reckless.

202. Plaintiffs and the North Carolina Statewide Class seek all available relief under N.C. Gen. Stat. §§ 75-16 and 75-16.1 including but not limited to injunctive relief, actual damages, treble damages, and attorneys' fees and costs

Claims Asserted on Behalf of the Nebraska Statewide Class

**COUNT XI —
Violation of the Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602;**

203. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

204. Plaintiffs Jackie L. Kier and Aloha Kier bring this cause of action on behalf of the Nebraska Statewide Class.

205. Equifax engages in "trade and commerce," as meant by Neb. Rev. Stat. § 59-1601, by selling credit-related services.

206. Equifax, while operating in Nebraska, engaged in unfair and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services in violation of Neb. Rev. Stat. § 59-1602, including but not limited to the following:

- Equifax misrepresented material facts to the Nebraska Statewide Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Nebraska Statewide Class members'

Personal Information from unauthorized disclosure, release, data breaches, and theft;

- Equifax misrepresented material facts to the Nebraska Statewide Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Nebraska Statewide Class members' Personal Information;
- Equifax suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Nebraska Statewide Class members' Personal Information;
- Equifax engaged in unfair acts and practices by failing to maintain the privacy and security of Nebraska Statewide Class members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, et seq.), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), the Nebraska Privacy of Insurance Consumer Information Act (Neb. Rev. Stat. §§ 44-910, 44-916), and the Nebraska Unfair Insurance Trade Practices Act (Neb. Rev. Stat. §§ 44-1524, 44-1425);
- Equifax engaged in unlawful and deceptive acts and practices by failing to disclose the Data Breach to Nebraska Statewide Class members in a timely and accurate manner, in violation of Neb. Rev. Stat. Ann. § 87-803(1);
- Equifax engaged in unlawful and deceptive acts and practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Nebraska Statewide Class members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

207. The above unlawful and deceptive acts and practices and acts by

Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused

substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

208. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Nebraska Statewide Class members' Personal Information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nebraska Statewide Class.

209. As a direct and proximate result of Defendant's unlawful practices, Nebraska Statewide Class members suffered injury and/or damages.

210. Nebraska Statewide Class members seek relief under Neb. Rev. Stat. § 59-1609, including, but not limited to, injunctive relief, actual damages, and attorneys' fees and costs.

**COUNT XII —
Violation of the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev.
Stat. § 87-302(a)(5) and (7), *et seq.***

211. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

212. Plaintiffs Jackie L. Kier and Aloha Kier bring this cause of action on behalf of the Nebraska Statewide Class.

213. Equifax, while operating in Nebraska, engaged in deceptive trade practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of credit-related services purchased by the Nebraska Statewide Class in violation of Neb. Rev. Stat. § 87-302, including but not limited to the following:

- Equifax misrepresented material facts to the Nebraska Statewide Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Nebraska Statewide Class members' Personal Information from unauthorized disclosure, release, data breaches, and theft in violation of Neb. Rev. Stat. § 87-302(5), (7), (9), (14), and (15);
- Equifax misrepresented material facts to the Nebraska Statewide Class by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Nebraska Statewide Class members' Personal Information in violation of Neb. Rev. Stat. § 87-302(5), (7), (9), (14), and (15);
- Equifax, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Nebraska Statewide Class members' Personal Information in violation of Neb. Rev. Stat. § 87-302(5), (7), (9), (14), and (15);
- Equifax engaged in deceptive trade practices by failing to maintain the privacy and security of Nebraska Statewide Class members' Personal Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These deceptive trade practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d, et seq.), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), the Nebraska Privacy of Insurance Consumer Information Act (Neb. Rev. Stat. §§ 44-910, 44-916), and the Nebraska Unfair Insurance Trade Practices Act (Neb. Rev. Stat. §§ 44-1524, 44-1425);

- Equifax engaged in deceptive trade practices by failing to disclose the Data Breach to Nebraska Statewide Class members in a timely and accurate manner, in violation of Neb. Rev. Stat. Ann. § 87-803(1);
- Equifax engaged in deceptive trade practices services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Nebraska Statewide Class members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

214. The above deceptive trade practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

215. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard Nebraska Statewide Class members' Personal Information and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nebraska Statewide Class.

216. As a direct and proximate result of Defendant's unlawful practices, Nebraska Statewide Class members suffered injury and/or damages, and will suffer future harm and/or damages as alleged in this Complaint.

217. Nebraska Statewide Class members seek relief under Neb. Rev. Stat. § 87-303, including, but not limited to, injunctive relief, other equitable relief, and attorneys' fees and costs.

Claims Asserted on Behalf of the Pennsylvania Statewide Class

**COUNT XIII —
Violation of the Pennsylvania Unfair Trade Practices and Consumer
Protection Law, 73 Pa. Stat. § 201-1, *et seq.***

218. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

219. Plaintiffs Larry Newcomer and Andrea Shafran bring this cause of action on behalf of the Pennsylvania Statewide Class.

220. Equifax and the Pennsylvania Statewide Class members are “persons” within the meaning of 73 Pa. Stat. Ann. § 201-2.(2).

221. Equifax is engaged in “trade” or “commerce” within the meaning of 73 Pa. Stat. Ann. § 201-2(3).

222. The Pennsylvania Unfair Trade Practices Act (“Pennsylvania UTPA”) prohibits “unfair or deceptive acts or practices in the conduct of any trade or commerce” 73 Pa. Stat. Ann. § 201 3.

223. In the course of its business, Equifax, through its agents, employees, and/or subsidiaries, violated the Pennsylvania UTPA as detailed above.

Specifically, Equifax engaged in unlawful, unfair, and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the services purchased by the Pennsylvania Statewide Class in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including but not limited to the following:

- Causing likelihood of confusion or of misunderstanding as to the security of consumer identifying information;
- Failing enact adequate privacy and security measures to protect the Pennsylvania Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;
- Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- Knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Pennsylvania Statewide Class members' PII from unauthorized disclosure, release, data breaches, and theft;
- Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for the Pennsylvania Statewide Class members' PII;
- Engaging in other conduct which created a likelihood of confusion or of misunderstanding; and/or
- Using or employing deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of a material fact with intent that others rely upon such concealment, suppression or omission, in connection with the advertisement and

sale of credit furnishing goods and services, whether or not any person has in fact been misled, deceived or damaged thereby.

224. Defendant's concealment of its data security shortcomings was material to Plaintiffs and the Pennsylvania Statewide Class, as Defendant intended. Had they known the truth, Plaintiffs and the Pennsylvania Statewide Class would have taken steps to prevent Equifax from obtaining their personal identifying information.

225. Plaintiffs and Pennsylvania Statewide Class members had no way of discerning that Defendant's representations were false and misleading, or otherwise learning the facts that Defendant had concealed or failed to disclose, because Defendant did not make public that information. Plaintiffs and Pennsylvania Statewide Class members did not, and could not, unravel Defendant's deception on their own.

226. Defendant had an ongoing duty to Plaintiffs and the Pennsylvania Statewide Class to refrain from unfair and deceptive practices under the UTPA in the course of their business. Specifically, Defendant owed Plaintiffs and Pennsylvania Statewide Class members a duty to disclose all the material facts concerning the measures taken to protect class members' sensitive information because they possessed exclusive knowledge, they intentionally concealed it from Plaintiffs and the Pennsylvania Statewide Class, and/or they made

misrepresentations that were rendered misleading because they were contradicted by withheld facts.

227. Plaintiffs and Pennsylvania Statewide Class members suffered ascertainable loss and actual damages as a direct and proximate result of Defendant's concealment, misrepresentations, and/or failure to disclose material information.

228. Defendant's violations present a continuing risk to Plaintiffs and the Pennsylvania Statewide Class, as well as to the general public. Defendant's unlawful acts and practices complained of herein affect the public interest.

229. Pursuant to 73 Pa. Stat. Ann. § 201-9.2(a), Plaintiffs and the Pennsylvania Statewide Class seek an order enjoining Defendant's unfair and/or deceptive acts or practices, and awarding damages, punitive and/or treble damages, and any other just and proper relief available under the Pennsylvania UTPA.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of members of the Nationwide Class and Statewide Classes, respectfully request:

230. An order certifying the proposed Class or Classes under the provisions of Rule 23 of the Federal Rules of Civil Procedure, and directing that notice be provided to all members of the Classes;

231. A finding that Equifax breached its duty to safeguard and protect the PII of Plaintiffs and Nationwide Class members that was compromised in the Data Breach;

232. Injunctive relief, including public injunctive relief in the form of an order enjoining Defendant from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

233. That Plaintiffs and Nationwide Class members recover damages in the form of restitution or disgorgement and/or compensatory damages for economic loss and out-of-pocket costs, treble damages under the applicable federal and state laws, and punitive and exemplary damages under applicable law;

234. A determination that Equifax is financially responsible for all Class notice and administration of Class relief;

235. A judgment against Defendant for any and all applicable statutory and civil penalties;

236. An order requiring Defendant to pay both pre- and post-judgment interest on any amounts awarded;

237. An award to Plaintiffs and Nationwide Class members of costs and reasonable attorneys' fees;

238. Leave to amend this Complaint to conform to the evidence produced in discovery and at trial; and

239. Such other or further relief as the Court may deem appropriate, just, and equitable.

VIII. DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable.

RESPECTFULLY SUBMITTED this 19th day of October, 2017.

MOTLEY RICE LLC

By: /s/ Kevin R. Dean

Kevin R. Dean (GA Bar #214855)

Joseph F. Rice, *pro hac vice forthcoming*

Jodi Flowers, *pro hac vice forthcoming*

Breanne Cope, *pro hac vice forthcoming*

28 Bridgeside Boulevard

Mount Pleasant, SC 29464

(843) 216-9000, Fax (843) 216-9450

kdean@motleyrice.com

jflowers@motleyrice.com

bcope@motleyrice.com

Laura Ray, *pro hac vice forthcoming*

Mathew Jasinski, *pro hac vice forthcoming*

One Corporate Center

20 Church Street

17th Floor

Hartford, CT 06103
(860) 882-1681, Fax (860) 882-1682
lray@motleyrice.com
mjasinski@motleyrice.com

Lynn Lincoln Sarko, *pro hac vice forthcoming*
Derek W. Loeser, *pro hac vice forthcoming*
Gretchen Freeman Cappio, *pro hac vice*
forthcoming
Cari Campen Laufenberg, *pro hac vice*
forthcoming

KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
(206) 623-1900, Fax (206) 623-3384
lsarko@kellerrohrback.com
dloeser@kellerrohrback.com
gcappio@kellerrohrback.com
claufenberg@kellerrohrback.com

Matthew J. Preusch, *pro hac vice forthcoming*
KELLER ROHRBACK L.L.P.
mpreusch@kellerrohrback.com
801 Garden Street, Suite 301
Santa Barbara, CA 93101
(805) 456-1496, Fax (805) 456-1497

Attorneys for Plaintiffs

CIVIL COVER SHEET

The JS44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

DORI M. MASHBURN, SARAH L. HARDY, RICHARD GAINES, VALERIE GAINES, JONATHAN C. ENTSMINGER, CARRIE L. ENTSMINGER JACKIE L. KIER, ALOHA KIER, LARRY NEWCOMER, and ANDREA SHAFRAN, Individually and on Behalf of All Others Similarly Situated

(b) COUNTY OF RESIDENCE OF FIRST LISTED

PLAINTIFF King County, WA
(EXCEPT IN U.S. PLAINTIFF CASES)

DEFENDANT(S)

EQUIFAX, INC., a Georgia Corporation

COUNTY OF RESIDENCE OF FIRST LISTED

DEFENDANT Fulton County, GA
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS

(FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

KEVIN R. DEAN
MOTLEY RICE LLC
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
(843) 216-9000, kdean@motleyrice.com

ATTORNEYS (IF KNOWN)**II. BASIS OF JURISDICTION**

(PLACE AN "X" IN ONE BOX ONLY)

- ☐ 1 U.S. GOVERNMENT PLAINTIFF
☐ 2 U.S. GOVERNMENT DEFENDANT
☐ 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
☒ 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES

(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

- | PLF | DEF | PLF | DEF |
|---------------------------------------|--|----------------------------|---|
| <input type="checkbox"/> 1 | <input type="checkbox"/> 1 CITIZEN OF THIS STATE | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE |
| <input checked="" type="checkbox"/> 2 | <input type="checkbox"/> 2 CITIZEN OF ANOTHER STATE | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE |
| <input type="checkbox"/> 3 | <input type="checkbox"/> 3 CITIZEN OR SUBJECT OF A FOREIGN COUNTRY | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 FOREIGN NATION |

IV. ORIGIN

(PLACE AN "X" IN ONE BOX ONLY)

- ☒ 1 ORIGINAL PROCEEDING
☐ 2 REMOVED FROM STATE COURT
☐ 3 REMANDED FROM APPELLATE COURT
☐ 4 REINSTATED OR REOPENED
☐ 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District)
☐ 6 MULTIDISTRICT LITIGATION - TRANSFER
☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
☐ 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION

(CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

Class Action Fairness Act, 28 U.S.C. § 1332(d)(2)
Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq.

(IF COMPLEX, CHECK REASON BELOW)

- | | |
|---|--|
| <input checked="" type="checkbox"/> 1. Unusually large number of parties. | <input type="checkbox"/> 6. Problems locating or preserving evidence |
| <input type="checkbox"/> 2. Unusually large number of claims or defenses. | <input checked="" type="checkbox"/> 7. Pending parallel investigations or actions by government. |
| <input type="checkbox"/> 3. Factual issues are exceptionally complex | <input type="checkbox"/> 8. Multiple use of experts. |
| <input type="checkbox"/> 4. Greater than normal volume of evidence. | <input type="checkbox"/> 9. Need for discovery outside United States boundaries. |
| <input checked="" type="checkbox"/> 5. Extended discovery period is needed. | <input type="checkbox"/> 10. Existence of highly technical issues and proof. |

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____	AMOUNT \$ _____	APPLYING IFP _____	MAG. JUDGE (IFP) _____
JUDGE _____	MAG. JUDGE _____ (Referral)	NATURE OF SUIT _____	CAUSE OF ACTION _____

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)CONTRACT - "0" MONTHS DISCOVERY TRACK

- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK

- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☐ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- ☐ 210 LAND CONDEMNATION
- ☐ 220 FORECLOSURE
- ☐ 230 RENT LEASE & EJECTMENT
- ☐ 240 TORTS TO LAND
- ☐ 245 TORT PRODUCT LIABILITY
- ☐ 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK

- ☐ 310 AIRPLANE
- ☐ 315 AIRPLANE PRODUCT LIABILITY
- ☐ 320 ASSAULT, LIBEL & SLANDER
- ☐ 330 FEDERAL EMPLOYERS' LIABILITY
- ☐ 340 MARINE
- ☐ 345 MARINE PRODUCT LIABILITY
- ☐ 350 MOTOR VEHICLE
- ☐ 355 MOTOR VEHICLE PRODUCT LIABILITY
- ☐ 360 OTHER PERSONAL INJURY
- ☐ 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- ☒ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☐ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK

- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK

- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK

- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK

- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK

- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK

- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK

- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK

- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK

- ☐ 830 PATENT
- ☐ 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDAs) - a/k/a Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK

- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK

- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK

- ☐ 375 FALSE CLAIMS ACT
- ☐ 376 Qui Tam 31 USC 3729(a)
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 490 CABLE/SATELLITE TV
- ☐ 890 OTHER STATUTORY ACTIONS
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK

- ☐ 410 ANTI-TRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK

- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23 DEMAND \$ _____ > \$5,000,000.00

JURY DEMAND ☒ YES ☐ NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE William S. Duffey, Jr. DOCKET NO. 1:2017-cv-03422

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)

- ☐ 1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- ☒ 2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- ☐ 3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- ☐ 4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.
- ☐ 5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.
- ☐ 6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):

☐ 7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. _____, WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.

/s/ Kevin R. Dean

October 19, 2017

SIGNATURE OF ATTORNEY OF RECORD

DATE