UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

NANCY M. VITA, HORACE C. RAMEY, JAMES A. BLACK, JIMMIE MOORE, THOMAS A. WILLIAMS, DANIEL R. DALTON, BRITTANY S. DALTON, individually and on behalf of all others similarly situated; Plaintiffs, v. EQUIFAX, INC., Defendant.	CIVIL ACTION FILE NO.:

CLASS ACTION COMPLAINT

Plaintiffs identified below (collectively "Plaintiffs"), individually and on behalf of the classes defined below of similarly situated persons ("Class Members"), allege against Defendant Equifax, Inc. ("Equifax") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents, the following:

PREAMBLE

1.

The system for protecting confidential personally identifiable information in corporate America is broken. Some companies use reliable data security practices and update those practices on a continuing basis to ensure the security of consumers' confidential personally identifiable information, medical information, and financial information ("PII"). Others do not. Over the last several years, hackers have breached the inadequate security systems of Target, Home Depot, Yahoo, Neiman Marcus, Nationwide, Anthem, Ashley Madison, eBay, JP Morgan Chase, Sony, Global Payments, Tricare, Citibank, Heartland, and even Experian (one of Equifax's competitors) in widely publicized cybersecurity incidents. Even so, Equifax continued to use inadequate data security practices, including vulnerable open source code in vital software the company used to both interact with the public and protect sensitive private information. The result was a foreseeable, and entirely preventable, data security breach that has severely harmed nearly one hundred and fifty million Americans, and will continue to harm them indefinitely into the future.

NATURE OF THE CASE

2.

The is a class action on behalf of a National Class of consumers, and subclasses of consumers residing in Georgia, Florida, South Carolina, and Tennessee, relating to a data breach of Equifax's computer systems that occurred during the period mid-May 2017 through July 29, 2017. This data breach affects over 140 million consumers, and is believed to be the largest data breach in U.S. history (the "Data Breach"). Plaintiffs bring claims pursuant to the Fair Credit Reporting Act, the Georgia Fair Business Practices Act, the Florida Deceptive and Unfair Trade Practices Act, the South Carolina Unfair Trade Practices Act, the South Carolina Breach of Security and Business Data Act, the Tennessee Consumer Protection Act, the Tennessee Data Breach Act, as well as common law claims of negligence, negligence per se, bailment, unjust enrichment, and breach of implied warranty. Plaintiffs also seek declaratory judgment and injunctive relief.

THE PARTIES

3.

Equifax is a multi-billion dollar Georgia corporation that provides credit information services to millions of businesses, governmental units, and

consumers across the globe. Equifax operates through various subsidiaries including Equifax Information Services, LLC, and Equifax Consumer Services, LLC a/k/a Equifax Personal Solutions a/k/a PSOL. Each of these entities, and Equifax's other affiliates, acted as agents of Equifax, or in the alternative, acted in concert with Equifax in relation to the activities alleged in this complaint.

4.

Nancy M. Vita is an individual consumer residing in Cobb County, Georgia. Upon information and belief, Ms. Vita's personal information was impacted by the Data Breach.

5.

Horace C. Ramey is an individual consumer residing in Rabun County, Georgia. Upon information and belief, Mr. Ramey's personal information was impacted by the Data Breach.

6.

James A. Black is an individual consumer residing in Cobb County, Georgia. Upon information and belief, Mr. Black's personal information was impacted by the Data Breach.

7.

Jimmie Moore is an individual consumer residing Palm Beach County, Florida. Upon information and belief, Mr. Moore's personal information was impacted by the Data Breach.

8.

Thomas A. Williams is an individual consumer residing in Hamilton County, Tennessee. Upon information and belief, Mr. Williams' personal information was impacted by the Data Breach.

9.

Daniel R. Dalton is an individual consumer residing in Charleston County, South Carolina. Upon information and belief, Mr. Dalton's personal information was impacted by the Data Breach.

10.

Brittany S. Dalton is an individual consumer residing in Charleston County, South Carolina. Upon information and belief, Ms. Dalton's personal information was impacted by the Data Breach.

JURISDICTION AND VENUE

11.

This Court has general and specific jurisdiction over Equifax and original

jurisdiction over Plaintiffs' claims.

12.

This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

13.

This Court has personal jurisdiction over Defendant because it maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Defendant Equifax intentionally avails itself to this jurisdiction by marketing and selling products and services from Georgia to millions of consumers nationwide, and the transactions and occurrences giving rise to this lawsuit occurred in Georgia.

14.

Venue is proper under 28 U.S.C. § 1391 because Equifax's principal place of business is in this District and a substantial part of the events, acts and omissions giving rise to Plaintiffs' claims occurred in this District.

STATEMENT OF FACTS

15.

During the period mid-May 2017 through July 29, 2017, credit reporting agency giant Equifax was subject to the largest data breach in U.S. history. Unauthorized persons penetrated a vulnerability in Equifax's United States website in order to gain access to the personal and financial information of approximately 143 million Americans. The information accessed includes names, Social Security numbers, birth dates, addresses, and driver's license numbers. Additionally, credit card numbers for approximately 209,000 U.S. consumers and dispute documents containing personal identifying information for roughly 182,000 U.S. consumers were accessed.

16.

Notwithstanding the scale and seriousness of the Data Breach, and despite its actual knowledge that Plaintiffs and other Class Members' PII was stolen, Equifax did not disclose this massive breach to the public until September 7, 2017, months after the theft had occurred. During this period of concealment, Equifax continued to accept monthly payments from security monitoring

customers while withholding information that the customers' PII had been stolen by hackers.

17.

Meanwhile, between July 29, 2017, when Equifax alleges that it first discovered the breach, and September 7, 2017, the date of public disclosure, Equifax executives sold at least $1.8 million worth of shares in company stock.

Equifax Has A History of Data Breaches.

18.

Upon information and belief, this is not the first data breach experienced by Equifax. For example, in March 2013, Equifax acknowledged that a hacker gained "fraudulent and unauthorized access" to PII of high profile persons including Michelle Obama and then FBI Director Robert Mueller.

19.

In 2016, a security researcher found a common vulnerability known as cross-site scripting (XSS) on the Equifax website, and this vulnerability allowed attackers to send specially-crafted links to Equifax customers and (if the links were clicked upon) provided hackers with customer usernames and passwords.

20.

In May 2016, Kroger announced to its employees that Equifax systems had been subject to a data breach in which the PII of 430,000 Kroger employees (including names, addresses, and Social Security numbers) maintained by Equifax had been compromised by hackers.

21.

In January 2017, Equifax announced a data leak in which credit information of customers at partner LifeLock had been exposed to another user of LifeLock's online portal.

22.

Prior to the subject Data Breach, Equifax had actual knowledge of the clear and present risks of immediate and continuing harm to victims of such data breaches. As described by Gasan Awad, former Vice President, Identity Fraud Product Management for Equifax, "[d]ata breaches are the first step for criminals with intentions to steal and misuse consumer information. Once fraudsters have consumers' private identity information they then take the next step in criminal activity, often committing fraud by opening fraudulent accounts or taking over an existing account. In essence, fraudsters use the personal information obtained

from the breaches to apply for credit or benefits or hijack existing accounts, all while acting as the victims."[1]

23.

Equifax, at all relevant times, was aware or should have been aware that the PII it collected and stored onto its systems is highly sensitive, subject to attack, and once accessed by third-parties, could be misused harming consumers.

24.

It has been widely publicized that companies such as Target, Home Depot, Yahoo, Neiman Marcus, Nationwide, Anthem, Ashley Madison, eBay, JP Morgan Chase, Sony, Global Payments, Tricare, Citibank, Heartland, and even Experian, one of Equifax's direct competitors, have been hacked by third-parties due to their inadequate security systems in place to safeguard against data breaches. Equifax knew or should have known about the frequent, previous data breaches.

25.

Plaintiffs bring this class action against Defendant Equifax for its failure to protect and secure consumers' personal and sensitive information and for its

[1] Awad, Gasan, *Device Advice: Keeping Fraudsters from Consumer Info*, http://www.darkreading.com/endpoint/device-advice-keeping-fraudsters-from-consumer-info/a/d-id/1325182 (last visited on 9/11/2017).

failure to provide consumers with timely and adequate notice that the Data Breach occurred, and the types of information that were stolen.

The Subject Data Breach was Massive.

26.

On September 7, 2017, Equifax first disclosed to the public that unauthorized persons exploited a website application vulnerability on one of the company's U.S.-based servers. This, in turn, exposed PII for approximately 143 million Americans.

27.

It is reported that the Data Breach occurred in the period May 2017 through July 29, 2017, the date when Equifax reports to have discovered it.

28.

The exposed data includes names, birth dates, Social Security numbers, addresses, and some driver's license numbers – the very kind of personal financial information Equifax is supposed to keep completely secure for its customers and for consumers.

29.

Approximately 209,000 U.S. credit card numbers were accessed in the Data Breach, as well as 182,000 credit report dispute documents that included

"personal identifying information."

30.

Despite the fact that Equifax believes the Data Breach occurred during the period May through July 2017, it waited months – until September 7, 2017 – to disclose the Data Breach to the public.

Equifax was Grossly Negligent and Reckless.

31.

Equifax knew or should have known about the ramifications for failing to maintain a sufficient security system designed to protect against data breaches of this very kind. Equifax also knew or should have known of the significant harm consumers, including Plaintiffs and Class Members, would suffer as a result of a data breach.

32.

Upon information and belief, the Data Breach is believed to have been perpetuated via the "Apache STRUTS flaw" in the software running Equifax's online databases.

33.

The Apache STRUTS flaw has been under attack by hackers since at least March 2017. Upon information and belief, the flaw had been successfully exploited by hackers prior to July 2017.

34.

An additional flaw in the Apache software utilized by Equifax involved the REST plugin, and has existed since 2008. Upon information and belief, the Apache REST flaw was an additional potential source of the subject Data Breach.

35.

Equifax used old technology, poor cybersecurity methods, out of date Java software, links in the source code to discontinued web browser Netscape, and vulnerable open source software without adequate security patches in connection with its public facing website. Equifax allowed its public facing website to be connected with its internal and (purportedly) secure internal databases containing customer and consumer PII, which, of course, increased the latter's vulnerability to hackers and data breaches.

36.

Despite its knowledge of the risk of a data breach, Equifax's attitude toward protecting and securing Plaintiffs' and Class Members' sensitive information was reckless, indifferent, and at the very least, negligent.

37.

The Data Breach was a direct and proximate result of Equifax's failure to adequately and sufficiently protect Plaintiffs' and Class Members' sensitive information from being accessed, used, sold, manipulated or disclosed.

38.

Although it had the resources to prevent a data breach, Equifax failed to implement and adopt procedures, software, systems and measures that could have prevented the Data Breach from occurring and instead, would have protected Plaintiffs' and Class Members' sensitive information.

It is well known that Data Breaches Cause Significant Harm.

39.

A 2012 Identity Fraud Report by Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, quantified the impact of data breaches and reported that individuals whose PII is subject to a reported

data breach—such as the subject Data Breach—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft.

40.

Moreover, there is a high probability that criminals who may now possess Plaintiffs' and the other Class Members' PII, but who have not yet used the information, will do so at a later date or re-sell such information. This probability is increased by Equifax's public statement that it will provide free monitoring services for affected consumers, but *only* for one year.

41.

The Federal Trade Commission ("FTC") states that "[i]dentity theft is a serious crime. It can disrupt your finances, credit history, and reputation, and take time, money, and patience to resolve."[2]

42.

Identity theft crimes often involve more than just crimes of financial loss, such as various types of government fraud (*e.g.*, obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using a victim's name and Social Security number to obtain government benefits; and/or filing a fraudulent tax return using a victim's information). Identity

[2] *See* https://www.consumer.ftc.gov/articles/pdf-0014-identity-theft.pdf.

thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments, and/or obtain medical services in a victim's name. Identity thieves also have been known to give a victim's PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

43.

According to the FTC, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and . . . any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[3] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[4]

[3] Protecting Consumer Privacy in an Era of Rapid Change FTC, Report March 2012 (http://www.ftc.gov/os/ 2012/03/120326privacyreport.pdf).

[4] Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report, 35-38 (Dec. 2010), available at http://www.ftc.gov/ os/2010/12/101201privacyreport.pdf; Comment of Center for Democracy & Technology, cmt. #00469, at 3; Comment of Statz, Inc., cmt. #00377, at 11-12.

44.

According to the Javelin Report, the mean consumer cost of rectifying identity fraud in 2011 was $354.00. The average fraud-related economic loss for such victims was $1,513.00. In 2011, the consumer cost for new account fraud and other fraud increased 33% and 50% respectively. Consumers who received a data breach notification had a fraud incidence rate of 19% in 2011.

45.

Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services, or goods. As of 2010, more than 50 million people in the United States did not have health insurance according to the U.S. census. This, in turn, has led to a surge in medical identity theft as a means of fraudulently obtaining medical care. Victims of medical identity theft also may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits.

46.

The Data Breach, and Defendant's untimely and inadequate notification of consumers regarding the Data Breach, also substantially increased Plaintiffs' and the other Class Members' risk of being victimized by "phishing." "Phishing" is

an attempt to acquire information (and sometimes, indirectly, money) such as usernames, passwords and credit card details by masquerading as a trustworthy entity through an electronic communication. *See* http://www.onguardonline.gov/articles/0003-phishing (last visited 9/11/17). Communications purporting to be from popular social websites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail spoofing or instant messaging, and often directs users to enter details at a fake website that looks and feels almost identical to the legitimate one. When criminals have access to PII from a large group of similarly situated victims, it is much more feasible to develop a believable phishing spoof email. They can then get this group of victims to reveal additional private information, such as credit cards, bank accounts, and the like.

47.

According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches, "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year *or more* before being used to commit identity theft. Further, once stolen data have been sold or posted

on the Web, fraudulent use of that information may *continue for years*." GAO, Report to Congressional Requesters, at p.33 (June 2007) (emphasis added), available at http://www.gao.gov/new.items/d07737.pdf (last visited 9/11/17). Accordingly, merely one year of credit monitoring, as offered by Equifax to affected consumers, is severely deficient to safeguard against the harm suffered by victims of a data breach.

Social Security Number Breaches
Cause Special Harm and Open-Ended Vulnerability.

48.

The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be replaced easily like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently or other damaging misuse. *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327 (http://www.ssa.gov/pubs/10064.html) (last accessed 9/11/17). Thus, a person whose PII has been stolen cannot obtain a new Social Security number until damage has already been done.

49.

Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems. For example, because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

50.

Because Social Security numbers are permanent identifying numbers associated with a person, the risk of harm to a victim of such theft is continuing and remains indefinitely. Whereas stolen credit cards can eventually be cancelled, a Social Security number is permanent. Unless the Social Security number is replaced (which can only occur *after* injury from identity fraud), the risk of identity fraud – and the value to criminals - continues year after year with no end.

Plaintiffs and Class Members Have Been Damaged.

51.

Defendant's wrongful actions and/or inactions and the resulting Data Breach have placed Plaintiffs and the other Class Members at an imminent, immediate and continuing increased risk of identity theft, identity fraud, and medical fraud.

52.

Consumers across the U.S. have suffered real and imminent harm as a result of Equifax's conduct, which includes (a) failing to implement adequate and reasonable measures to ensure its data systems were secure and protected; (b) failing to take available steps to prevent the Data Breach from occurring; (c) failing to disclose to its customers, consumers, and the public in general that it did not have adequate technology, computer systems and security practices to safeguard consumers' personal and financial information; and (d) failing to provide timely and adequate notice of the Data Breach.

53.

Defendant's wrongful actions and/or inactions and the resulting Data Breach have placed Plaintiffs and the Class Members at imminent, immediate, and continuing increased risk of identity theft, identity fraud, and medical fraud.

Identity theft occurs when someone uses an individual's PII, such as the person's name, Social Security number, or credit card number, without the individual's permission, to commit fraud or other crimes. *See* http://www.consumer.ftc.gov/articles/pdf-0014-identity-theft.pdf (last visited on 9/11/17).[5]

54.

Plaintiffs and members of the national and state classes have also suffered imminent and impending injury arising from a serious and increased risk of fraud, identity fraud, misuse of their personal information, annoyance, loss of productivity, and emotional distress, among other injuries.

55.

Plaintiffs and Class Members maintain a continuing interest in ensuring that their personal and sensitive information, which remains in the possession of Equifax, is protected and secured from future breaches.

[5] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, inter alia, credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

56.

Consumers' personal and financial information is invaluable and makes consumers vulnerable to further criminal harm. For example, a combination of one's Social Security number and date of birth may allow identity thieves to impersonate the consumer victim. Moreover, such information enables identity thieves and other criminals to open bank accounts and apply for loans, credit cards, housing, government benefits, and utilities in the consumer victim's name.

57.

Thieves may also sell the consumer victim's information to others.

58.

Identity thieves may get medical services using consumers' compromised personal information. Most victims who have had their information used for fraudulent purchases spent more than a month attempting to resolve problems. In comes cases, it can take years.

59.

Identity thieves can use personal identifying information to file tax returns and obtain fraudulent tax refunds in the victim's name.

60.

Once a consumer's personal and financial information is released onto the

internet black market, the consumer could be at risk of fraud and identity theft for years into the future.

61.

Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their personal and financial information.

62.

Importantly, Equifax did not obtain Plaintiffs' and Class Members' consent to disclose their personal and financial information to any other person as required by applicable law and industry standards.

63.

As a direct and proximate result of Equifax's said failures and the resulting Data Breach, Plaintiffs and Class Members have been and will continue to be subject to an imminent, immediate, and increased risk of harm from identity theft and fraud, requiring them to take time and devote resources toward monitoring and mitigating the actual and potential impacts of the Data Breach.

64.

Upon information and belief, Plaintiffs and Class Members are therefore entitled to recover economic damages for harms including but not limited to:

a. Trespass, damage to and theft of their personal property including personal and financial information;

b. Improper disclosure of their personal and financial information;

c. The imminent and impending injury flowing from potential fraud and identity theft posed by their personal and financial information;

d. Unauthorized charges on their debit and credit card accounts;

e. Identity theft and fraud;

f. Information being placed in the hands of criminals and having been already misused via the sale of such information on the Internet black market;

g. Damages flowing from Equifax's untimely and inadequate notification of the Data Breach;

h. Loss of privacy suffered as a result of the Data Breach;

i. Ascertainable losses in the form of out-of-pocket expenses and the value of time reasonably incurred to remedy or mitigate the effects of the Data Breach;

j. Ascertainable losses in the form of deprivation of the value of their personal and financial information for which there is a well-established and quantifiable national and international market;

k. The loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts; and

l. The loss of productivity and value of their time spent to address, to attempt to ameliorate, to mitigate, and to deal with actual and future consequences of the Data Breach.

65.

To date, Equifax has not offered to consumers meaningful credit-monitoring or identity theft protection services. A conditional offer of non-immediate one year of monitoring by Equifax is inadequate for a breach of this size and scope that includes disclosure of Social Security numbers. Some Plaintiffs and Class Members understandably do not wish to entrust monitoring for identity theft to the very entity that exposed them to the risk of identity theft in the first place. And, even for those willing to entrust this responsibility to Equifax, the real, imminent, and continuing risk unfortunately extends beyond

one year. Criminals stealing or purchasing PII associated with this hack can also read the public statement Equifax has issued offering only one year of monitoring services, and can sensibly sell or use their ill-gotten PII after the expiration of this one year period. Accordingly, Plaintiffs and the Class Members are entitled to indefinite and continuing monitoring along with comprehensive identity theft insurance that covers the substantial and varied harms flowing from theft of a person's identity.

66.

In response to the Data Breach, Plaintiff James Black has taken and continues to take steps to protect his identity and his PII, including but not limited to purchasing the Identity Guard Total Protection Plan at a cost of $19.99 per month.

67.

In response to the Data Breach, Plaintiff Nancy Vita has taken and continues to take reasonable steps to protect her identity and her PII, including but not limited to purchasing a Transunion and Experian credit freeze for $3.00 each.

68.

Prior to the Data Breach and during the period that Equifax concealed the existence of the Data Breach, Ms. Vita was a customer of Equifax security monitoring software. Equifax willfully concealed the existence of the Data Breach from Ms. Vita for at least one month after the Data Breach discovery, while continuing to accept payment for security monitoring from Ms. Vita.

69.

In response to the Data Breach, Plaintiff Horace Ramey has taken and continues to take reasonable steps to protect his identity and his PII, including but not limited to purchasing a credit freeze and identity theft protection program.

70.

In response to the Data Breach, Plaintiff Jimmie Moore has taken and continues to take reasonable steps to protect his identity and his PII, including but not limited to purchasing Identity Guard Total Protection Plan at a cost of $19.99 per month.

71.

In response to the Data Breach, Plaintiff Daniel Dalton has taken and continues to take reasonable steps to protect his identity and his PII, including

but not limited to purchasing the Lifelock Protection Plan at a cost of $26.99 per month, and purchasing a Transunion and Experian credit freeze.

72.

In response to the Data Breach, Plaintiff Brittany Dalton has taken and continues to take reasonable steps to protect her identity and her PII, including but not limited to purchasing the Lifelock Protection Plan at a cost of $26.99 per month, and purchasing a Transunion and Experian credit freeze.

73.

In response to the Data Breach, Plaintiff Thomas Williams has taken and continues to take reasonable steps to protect his identity and his PII, including but not limited to purchasing an identity protection service.

CLASS ALLEGATIONS

I. The National Class

74.

Pursuant to Fed. R. Civ. P. 23, all Plaintiffs assert claims for violation of the Fair Credit Reporting Act, the Georgia Fair Business Practices Act, and common law claims of negligence, negligence per se, bailment, unjust enrichment, breach of implied warranty, declaratory judgment, and injunctive relief on behalf of a national class, defined as follows:

> All residents of the United States whose PII was accessed without authorization or was compromised as a result of the Data Breach (the "National Class").

75.

Excluded from the National Class are Equifax and its affiliates, parents or subsidiaries; all employees of Equifax; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

76.

The National Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and (c)(4).

Fed. R. Civ. P. 23(a).

77.

Numerosity. The National Class includes over 100 million consumers whose data was compromised in the Data Breach. The massive size of the Data Breach indicates that joinder of each member would be impracticable. Class Members may be identified through objective means. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

78.

Commonality. Common questions of law and fact exist and predominate over any questions affecting only individual Class Members. The common questions include:

a. whether Equifax violated the Fair Credit Reporting Act relating to the breach, concealment and then notice of the breach, the inadequate security measures taken to protect consumer PII from the breach, and notice to consumers of inadequate security;

b. whether Equifax had a legal duty to adequately protect Plaintiffs' and Class Members' PII;

c. whether Equifax breached its legal duty by failing to adequately protect Plaintiffs' and Class Members' PII;

d. whether Equifax had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

e. whether Equifax breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

f. whether and when Equifax knew or should have known that Plaintiffs' and Class Members' PII stored on its computer systems was vulnerable to attack;

g. whether Plaintiffs and Class Members are entitled to recover actual damages and/or statutory damages; and

h. whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

79.

Typicality. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and Class Members were injured through Equifax's uniform misconduct and their legal claims arise from the same core Equifax practices.

80.

Adequacy. Plaintiffs are adequate representatives of the proposed classes because their interests do not conflict with the interests of the Class Members they seek to represent. Plaintiffs' counsel are experienced in litigating consumer class actions and complex disputes.

81.

Superiority. A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Equifax. Even

if it were economically feasible, requiring millions of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

Fed. R. Civ. P. 23(b)(2).

82.

Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Equifax has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

Fed. R. Civ. P. 23(b)(3).

83.

There are questions of law and fact common to the National Class that under Fed. R. Civ. P. 23(b)(3) predominate over any questions solely affecting individual members of the National Class, including but not limited to those common questions of law and fact identified in paragraph No. 78(a-h).

Fed. R. Civ. P. 23(c)(4).

84.

Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the same issues identified in paragraph No. 78(a-h).

II. The Georgia Class.

85.

Pursuant to Fed. R. Civ. P. 23, Plaintiffs Vita, Ramey, and Black assert claims for violation of the Georgia Fair Business Practices Act, and common law claims of negligence, negligence per se, bailment, unjust enrichment, breach of implied warranty, declaratory judgment, and injunctive relief on behalf of a Georgia class, defined as follows:

> All residents of the state of Georgia whose PII was accessed without authorization or was compromised as a result of the Data Breach (the "Georgia Class").

86.

Excluded from the Georgia Class are Equifax and its affiliates, parents or subsidiaries; all employees of Equifax; all persons who make a timely election to

be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

87.

The Georgia Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and (c)(4):

Fed. R. Civ. P, 23(a).

88.

Numerosity. The Georgia Class includes over one million consumers whose data was compromised in the Data Breach. The massive size of the Data Breach indicates that joinder of each member would be impracticable. Georgia Class Members may be identified through objective means. Georgia Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

89.

Commonality. Common questions of law and fact exist and predominate over any questions affecting only individual Georgia Class Members. The common questions include:

a. whether Equifax violated the Georgia Fair Business Practices Act, O.C.G.A. §§ 10-1-393(a) and (b)(2), (3), (5), and (7), relating to the breach, concealment and then notice of the breach, the inadequate security measures taken to protect consumer PII from the breach, and notice to consumers of inadequate security;

b. whether Equifax had a legal duty to adequately protect Plaintiffs' and Class Members' PII;

c. whether Equifax breached its legal duty by failing to adequately protect Plaintiffs' and Class Members' PII;

d. whether Equifax had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

e. whether Equifax breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

f. whether and when Equifax knew or should have known that Plaintiffs' and Class Members' PII stored on its computer systems was vulnerable to attack;

g. whether Plaintiffs and Class Members are entitled to recover actual damages and/or statutory damages; and

h. whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

90.

Typicality. Plaintiffs Vita, Ramey, and Black's claims are typical of the claims of the Georgia Class. Plaintiffs and Georgia Class Members were injured through Equifax's uniform misconduct and their legal claims arise from the same core Equifax practices.

91.

Adequacy. Plaintiffs Vita, Ramey, and Black are adequate representatives of the proposed classes because their interests do not conflict with the interests of the Georgia Class Members they seek to represent. Plaintiffs' counsel are very experienced in litigating consumer class actions and complex disputes.

92.

Superiority. A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Georgia Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Equifax. Even if it were economically feasible, requiring millions of injured

plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

Fed. R. Civ. P. 23(b)(2).

93.

Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Equifax has acted or has refused to act on grounds generally applicable to the Georgia Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Georgia Class as a whole.

94.

There are questions of law and fact common to the Georgia Class under Fed. R. Civ. P. 23(b)(3) that predominate over any questions solely affecting individual members of the Georgia Class, including but not limited to those common questions of law and fact identified in paragraph No. 89(a-h).

Fed. R. Civ. P. 23(c)(4).

95.

Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the same issues identified in paragraph No. 89(a-h).

III. The Florida Class.

96.

Pursuant to Fed. R. Civ. P. 23, Plaintiff Jimmie Moore assert claims for violation of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), and common law claims of negligence, negligence per se, bailment, unjust enrichment, breach of implied warranty, declaratory judgment, and injunctive relief on behalf of a Florida class, defined as follows:

> All residents of the state of Florida whose PII was accessed without authorization or was compromised as a result of the Data Breach (the "Florida Class").

97.

Excluded from the Florida Class are Equifax and its affiliates, parents or subsidiaries; all employees of Equifax; all persons who make a timely election to

be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

98.

The Florida Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and (c)(4):

Fed. R. Civ. P. 23(a).

99.

Numerosity. The Florida Class includes over one million consumers whose data was compromised in the Data Breach. The massive size of the Data Breach indicates that joinder of each member would be impracticable. Florida Class Members may be identified through objective means. Florida Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

100.

Commonality. Common questions of law and fact exist and predominate over any questions affecting only individual Florida Class Members. The common questions include:

a. whether Equifax violated the FDUTPA relating to the breach, concealment and then notice of the breach, the inadequate security measures taken to protect consumer PII from the breach, and notice to consumers of inadequate security;

b. whether Equifax had a legal duty to adequately protect Plaintiffs' and Class Members' PII;

c. whether Equifax breached its legal duty by failing to adequately protect Plaintiffs' and Class Members' PII;

d. whether Equifax had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

e. whether Equifax breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

f. whether and when Equifax knew or should have known that Plaintiffs' and Class Members' PII stored on its computer systems was vulnerable to attack;

g. whether Plaintiffs and Class Members are entitled to recover actual damages and/or statutory damages;

h. whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust; and

i. what security procedures and data-breach notification procedures should Equifax be required to implement as part of any injunctive relief ordered by the Court.

101.

Typicality. Plaintiff Jimmie Moore's claims are typical of the claims of the Florida Class. Plaintiff Moore and Florida Class Members were injured through Equifax's uniform misconduct and their legal claims arise from the same core Equifax practices.

102.

Adequacy. Plaintiff Jimmie Moore is an adequate representative of the proposed classes because his interests do not conflict with the interests of the Florida Class Members he seeks to represent. Plaintiff's counsel are very experienced in litigating consumer class actions and complex disputes.

103.

Superiority. A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each

Florida Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Equifax. Even if it were economically feasible, requiring millions of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

Fed. R. Civ. P. 23(b)(2).

104.

Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Equifax has acted or has refused to act on grounds generally applicable to the Florida Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Florida Class as a whole.

Fed. R. Civ. P. 23(b)(3).

105.

There are questions of law and fact common to the Florida Class under Fed. R. Civ. P. 23(b)(3) that predominate over any questions solely affecting

individual members of the Florida Class, including but not limited to those common questions of law and fact identified in paragraph No. 100(a-i).

Fed. R. Civ. P. 23(c)(4).

106.

Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the same issues identified in paragraph No. 100(a-i).

IV. The South Carolina Class.

107.

Pursuant to Fed. R. Civ. P. 23, Plaintiffs B. Dalton and D. Dalton assert claims for violation of the South Carolina Unfair Trade Practices Act ("SCUTPA"), S.C. Code Ann. § 39-5-10, *et seq.*, and Breach of Security and Business Data Act ("BSBDA"), S.C. Code Ann. § 39-1-90(A), *et seq.*; and common law claims of negligence, negligence per se, bailment, unjust enrichment, breach of implied warranty, declaratory judgment, and injunctive relief on behalf of a South Carolina class, defined as follows:

> All residents of the state of South Carolina whose PII was accessed without authorization or was compromised as a result of the Data Breach (the "South Carolina Class").

108.

Excluded from the South Carolina Class are Equifax and its affiliates, parents or subsidiaries; all employees of Equifax; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

109.

The South Carolina Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and (c)(4):

Fed. R. Civ. P. 23(a).

110.

Numerosity. The South Carolina Class includes over one million consumers whose data was compromised in the Data Breach. The massive size of the Data Breach indicates that joinder of each member would be impracticable. South Carolina Class Members may be identified through objective means. South Carolina Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

111.

Commonality. Common questions of law and fact exist and predominate over any questions affecting only individual South Carolina Class Members. The common questions include:

a. whether Equifax violated the SCUTPA relating to the breach, concealment and then notice of the breach, the inadequate security measures taken to protect consumer PII from the breach, and notice to consumers of inadequate security;

b. whether Equifax violated the BSBDA;

c. whether Equifax had a legal duty to adequately protect Plaintiffs' and Class Members' PII;

d. whether Equifax breached its legal duty by failing to adequately protect Plaintiffs' and Class Members' PII;

e. whether Equifax had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

f. whether Equifax breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

g. whether and when Equifax knew or should have known that Plaintiffs' and Class Members' PII stored on its computer systems was vulnerable to attack;

h. whether Plaintiffs and Class Members are entitled to recover actual damages and/or statutory damages;

i. whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust; and

j. what security procedures and data-breach notification procedures should Equifax be required to implement as part of any injunctive relief ordered by the Court.

112.

Typicality. Plaintiffs B. Dalton and D. Dalton's claims are typical of the claims of the South Carolina Class. Plaintiffs D. Dalton and B. Dalton and South Carolina Class Members were injured through Equifax's uniform misconduct and their legal claims arise from the same core Equifax practices.

113.

Adequacy. Plaintiffs B. Dalton and D. Dalton are adequate representatives of the proposed classes because their interests do not conflict with the interests

of the South Carolina Class Members they seek to represent. Plaintiffs' counsel are very experienced in litigating consumer class actions and complex disputes.

114.

Superiority. A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each South Carolina Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Equifax. Even if it were economically feasible, requiring millions of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

Fed. R. Civ. P. 23(b)(2).

115.

Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Equifax has acted or has refused to act on grounds generally applicable to the South Carolina Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the South Carolina Class as a whole.

Fed. R. Civ. P. 23(b)(3).

116.

There are questions of law and fact common to the South Carolina Class under Fed. R. Civ. P. 23(b)(3) that predominate over any questions solely affecting individual members of the South Carolina Class, including but not limited to those common questions of law and fact identified in paragraph No. 111(a-j).

Fed. R. Civ. P. 23(c)(4).

117.

Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the same issues identified in paragraph No. 111(a-j).

V. The Tennessee Class.

118.

Pursuant to Fed. R. Civ. P. 23, Plaintiff Thomas A. Williams asserts claims for violation of the Tennessee Consumer Protection Act ("TCPA"), Tenn. Code. Ann. §§ 47-18-104, *et seq.*, and Tennessee Data Breach Act, Tenn. Code. Ann.

§§ 47-18-2107(b), *et seq.* and common law claims of negligence, negligence per se, bailment, unjust enrichment, breach of implied warranty, declaratory judgment, and injunctive relief of a Tennessee class, defined as follows:

> All residents of the state of Tennessee whose PII was accessed without authorization or was compromised as a result of the Data Breach (the "Tennessee Class").

119.

Excluded from the Tennessee Class are Equifax and its affiliates, parents or subsidiaries; all employees of Equifax; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

120.

The Tennessee Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and (c)(4):

Fed. R. Civ. P. 23(a).

121.

Numerosity. The Tennessee Class includes over one million consumers whose data was compromised in the Data Breach. The massive size of the Data Breach indicates that joinder of each member would be impracticable. Tennessee Class Members may be identified through objective means. Tennessee Class

Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

122.

Commonality. Common questions of law and fact exist and predominate over any questions affecting only individual Tennessee Class Members. The common questions include:

a. whether Equifax violated the TCPA relating to the breach, concealment and then notice of the breach, the inadequate security measures taken to protect consumer PII from the breach, and notice to consumers of inadequate security;

b. whether Equifax violated the Tennessee Data Breach Act, Tenn. Code. Ann. §§ 47-18-2107(b), *et seq.*

c. whether Equifax had a legal duty to adequately protect Plaintiffs' and Class Members' PII;

d. whether Equifax breached its legal duty by failing to adequately protect Plaintiffs' and Class Members' PII;

e. whether Equifax had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

f. whether Equifax breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

g. whether and when Equifax knew or should have known that Plaintiffs' and Class Members' PII stored on its computer systems was vulnerable to attack;

h. whether Plaintiffs and Class Members are entitled to recover actual damages and/or statutory damages;

i. whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust; and

j. what security procedures and data-breach notification procedures should Equifax be required to implement as part of any injunctive relief ordered by the Court.

123.

Typicality. Plaintiff Williams' claims are typical of the claims of the Tennessee Class. Plaintiff Williams and Tennessee Class Members were injured through Equifax's uniform misconduct and their legal claims arise from the same core Equifax practices.

124.

Adequacy. Plaintiff Williams is an adequate representative of the proposed classes because his interests do not conflict with the interests of the Tennessee Class Members they seek to represent. Plaintiffs' counsel are very experienced in litigating consumer class actions and complex disputes.

125.

Superiority. A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Tennessee Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Equifax. Even if it were economically feasible, requiring millions of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

Fed. R. Civ. P. 23(b)(2).

126.

Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). Equifax has acted or has refused to act on grounds generally applicable to the Tennessee Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Tennessee Class as a whole.

Fed. R. Civ. P. 23(b)(3).

127.

There are questions of law and fact common to the Tennessee Class under Fed. R. Civ. P. 23(b)(3) that predominate over any questions solely affecting individual members of the Tennessee Class, including but not limited to those common questions of law and fact identified in paragraph No. 122(a-j).

Fed. R. Civ. P. 23(c)(4).

128.

Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the same issues identified in paragraph No. 122(a-j).

COUNT I- NEGLIGENCE (ON BEHALF OF PLAINTIFFS AND THE NATIONAL, GEORGIA, FLORIDA, SOUTH CAROLINA, AND TENNESSEE CLASSES)

129.

Plaintiffs reallege, as if fully set forth, the allegations of paragraphs Nos. 1-128 above.

130.

Equifax owed duties of reasonable care to Plaintiffs and members of the National Class and Georgia Class, Florida Class, South Carolina Class and Tennessee Class (collectively, the "Classes" as used in this Count).

131.

Equifax's duties of care included duties:

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

b. to maintain procedures to prevent against PII data breaches and discovery such breaches;

c. to disclose to consumers that PII data had been breached;

d. to disclose to consumers that their PII data was not adequately secured to prevent a breach; and

e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Class Members of the Data Breach.

132.

Equifax knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Equifax received warnings from within and outside the company that hackers routinely attempted to access PII without authorization. Equifax also knew about numerous, well-publicized data breaches by other national companies.

133.

Equifax knew, or should have known, that its computer systems did not adequately safeguard Plaintiffs' and Class Members' PII.

134.

Because Equifax knew that a breach of its systems would damage millions of consumers, including Plaintiffs and Class Members, it had a duty to adequately protect their PII.

135.

Equifax had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Equifax with their PII was

predicated on the understanding that Equifax would take adequate security precautions. Moreover, only Equifax had the ability to protect its systems and the PII it stored on them from attack.

136.

Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PII. Equifax's misconduct included failing to implement the systems, policies, and procedures necessary to prevent this type of data breach.

137.

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

138.

Equifax breached the duties it owed to Plaintiffs and Class Members in numerous ways, including but not limited to:

a. by creating a foreseeable risk of harm through the misconduct previously described;

b. by failing to implement adequate security systems, protocols and practices sufficient to protect their PII both before and after learning of the Data Breach;

c. by failing to comply with the minimum industry data security standards during the period of the Data Breach; and

d. by failing to timely and accurately disclose to consumers that their PII had been improperly acquired or accessed.

139.

But for Equifax's wrongful and negligent breach of the duties it owed Plaintiffs and Class Members, their PII either would not have been compromised or they would have been able to prevent some or all of their damages.

140.

Equifax's breached the aforesaid duties which are imposed by the common laws of Georgia, Florida, South Carolina, Tennessee, and all other states. The breach of such duties damaged members of the National, Georgia, Florida, South Carolina, and Tennessee classes.

141.

The injury and harm that Plaintiffs and Class Members suffered (as alleged above) was the direct and proximate result of Equifax's negligent conduct.

Accordingly, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II- NEGLIGENCE PER SE (ON BEHALF OF PLAINTIFFS AND THE NATIONAL, GEORGIA, FLORIDA, SOUTH CAROLINA, AND TENNESSEE CLASSES)

142.

Plaintiffs reallege, as if fully set forth, the allegations of paragraphs Nos. 1-141 above.

143.

Section 5 of the FTC Act prohibits "unfair….practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

144.

Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards.

145.

Equifax's violation of Section 5 of the FTC Act constitutes negligence per se.

146.

Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

147.

The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to safeguard against.

148.

As a direct and proximate result of Equifax's negligence per se, Plaintiffs and Class Members have suffered, and continue to suffer, damages arising from Plaintiffs' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees and foregone cash back rewards and damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and

detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT III- BREACH OF IMPLIED CONTRACT (ON BEHALF OF PLAINTIFF VITA AND THE NATIONAL, GEORGIA, FLORIDA, SOUTH CAROLINA, AND TENNESSEE CLASSES)

149.

Plaintiffs reallege, as if fully set forth, the allegations of paragraphs Nos. 1-148 above.

150.

When Plaintiff Vita and Class Members provided their PII to Equifax in purchasing Equifax's products and services, they entered into implied contracts by which Equifax agreed to protect their PII and timely notify them in the event of a data breach.

151.

Equifax invited its customers, including Plaintiffs and Class Members, to purchase Equifax's products and services using credit and debit cards in order to increase sales by making purchases more convenient. The PII also was valuable to Equifax, because Equifax uses it for business and marketing purposes.

152.

An implicit part of the offer was that Equifax would safeguard the PII using reasonable or industry-standard means and would timely notify Plaintiffs and Class Members in the event of a data breach.

153.

Equifax affirmatively represented that it collected its customers' PII when they used and/or purchased Equifax's products and services, used that information for a variety of business purposes, and protected the PII using "industry standard means."

154.

Based on the implicit understanding and also on Equifax's representations, Plaintiffs and Class Members accepted the offers and provided Equifax with their PII by using their credit or debit cards in connection with purchases made during the period of the Data Breach.

155.

Plaintiffs and Class Members would not have provided their PII to Equifax had they known that Equifax would not safeguard their PII as promised or provide timely notice of a data breach.

156.

Plaintiffs and Class Members fully performed their obligations under the

implied contracts with Equifax.

157.

Equifax breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and failing to provide them with timely and accurate notice when their PII was compromised in the Data Breach.

158.

The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Equifax's breaches of its implied contracts with them.

COUNT IV- WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA") (ON BEHALF OF PLAINTIFFS AND THE NATIONAL, GEORGIA, FLORIDA, SOUTH CAROLINA, AND TENNESSEE CLASSES)

159.

Plaintiffs reallege, as if fully set forth, the allegations of paragraphs Nos. 1-158 above.

160.

Plaintiffs and Class Members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

161.

Under the FCRA, a "consumer reporting agency" is defined as "any person

which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f).

162.

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

163.

The FCRA requires Equifax to "maintain reasonable procedures designed to….limit the furnishing of consumer reports to the purposes listed under Section 1681b of this title." 15 U.S.C. § 1681e(a).

164.

Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character,

general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under Section 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Plaintiffs' and Class Members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing Plaintiffs' and Class Members' eligibility for credit.

165.

As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed Class Members' PII. Equifax violated § 1681b by furnishing consumer

reports to unauthorized or unknown entities or computer hackers, as detailed above.

166.

Equifax furnished Class Members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

167.

"Medical information" means "information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to. . . the payment for the provision of health care to an individual." 15 U.S.C. § 1681a(i).

168.

Equifax furnished Class Members' medical information by disclosing their medical information to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their medical information;

knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their medical information; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their medical information.

169.

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

170.

Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under Section 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, Equifax's numerous 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 such measures.

171.

Equifax also acted willfully and recklessly 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 FTC. *See*, e.g., 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted willfully and knowingly 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.

172.

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

173.

Plaintiffs and the National Class Members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the National Class Members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

174.

Plaintiffs and the National Class Members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. §1681n(a)(2)& (3).

COUNT V- NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT (ON BEHALF OF PLAINTIFFS AND THE NATIONAL, GEORGIA, FLORIDA, SOUTH CAROLINA, AND TENNESSEE CLASSES)

175.

Plaintiffs reallege, as if fully set forth, the allegations of paragraphs Nos. 1-174 above.

176.

Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under Section 1681b of the FCRA. Equifax's negligent failure to maintain

reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous 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 such measures.

177.

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

178.

Plaintiffs and the National Class member have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the National Class member are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

179.

Plaintiffs and the National Class member are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT VI- VIOLATION OF GEORGIA FAIR BUSINESS PRACTICES ACT O.C.G.A. § 10-1-390, ET SEQ. (ON BEHALF GEORGIA PLAINTIFFS AND THE NATIONAL CLASS)

180.

Georgia Plaintiffs reallege, as if fully set forth, the allegations of paragraphs Nos. 1-179 above.

181.

Equifax is engaged in, and their acts and omissions affect, trade and commerce pursuant to O.C.G.A. § 10-1-392(28).

182.

As discussed above, Equifax's acts, practices, and omissions at issue in this matter were directed and emanated from its headquarters in Georgia.

183.

The Georgia Plaintiffs and National Class Members entrusted Equifax with their PII.

184.

As alleged herein this Complaint, Equifax engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the Georgia Fair Business Practices Act ("GFBPA"):

a. failure to maintain adequate computer systems and data security practices to safeguard PII;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to timely and accurately disclose the Data Breach to Georgia Plaintiffs and National Class Members;

d. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the Data Breach and before it allegedly remediated the breach.

185.

Furthermore, as alleged above, Equifax's failure to secure consumers' PII violated the FTCA and therefore violated the GFBPA.

186.

Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Georgia Plaintiffs and

National Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

187.

As a direct and proximate result of Equifax's violation of the GFBPA, Georgia Plaintiffs and National Class Members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Georgia Plaintiffs and National Class Members; damages arising from Georgia Plaintiffs' and National Class Members' inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards and damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching,

adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

188.

Also as a direct result of Equifax's knowing violation of the GFBPA, Georgia Plaintiffs and National Class Members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Equifax segment PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. Ordering that Equifax purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Equifax conduct regular database scanning and securing checks;

g. Ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Equifax to meaningfully educate consumers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps consumers should take to protect themselves.

189.

Georgia Plaintiffs bring this action on behalf of themselves and Georgia Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to

allow consumers to make informed purchasing decisions and to protect Georgia Plaintiffs and National Class Members and the public from Equifax's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Equifax's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

190.

Georgia Plaintiffs and National Class Members are entitled to a judgment against Equifax for actual and consequential damages, exemplary damages and attorneys' fees pursuant to the GFBPA, costs, and such other further relief as the Court deems just and proper.

COUNT VII- VIOLATION OF GEORGIA FAIR BUSINESS PRACTICES ACT O.C.G.A. § 10-1-390, ET SEQ. (ON BEHALF OF GEORGIA PLAINTIFFS AND THE GEORGIA CLASS)

191.

Georgia Plaintiffs reallege, as if fully set forth, the allegations of paragraphs Nos. 1-190 above.

192.

Equifax is engaged in, and their acts and omissions affect, trade and commerce pursuant to O.C.G.A. § 10-1-392(28).

193.

As discussed above, Equifax's acts, practices, and omissions at issue in this matter were directed and emanated from its headquarters in Georgia.

194.

Georgia Plaintiffs and Georgia Class Members entrusted Equifax with their PII.

195.

As alleged herein this Complaint, Equifax engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the GFBPA:

a. failure to maintain adequate computer systems and data security practices to safeguard PII;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to timely and accurately disclose the Data Breach to Georgia Plaintiffs and Georgia Class Members;

d. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the Data Breach and before it allegedly remediated the Breach.

196.

Furthermore, as alleged above, Equifax's failure to secure consumers' PII violates the FTCA and therefore violates the GFBPA.

197.

Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Georgia Plaintiffs and Georgia Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

198.

As a direct and proximate result of Equifax's violation of the GFBPA, Georgia Plaintiffs and Georgia Class Members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Georgia Plaintiffs and Georgia Class Members; damages arising from Plaintiffs' inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as

a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards and damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

199.

Also as a direct result of Equifax's knowing violation of the GFBPA, Georgia Plaintiffs and Georgia Class Members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to

conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Equifax segment PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. Ordering that Equifax purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Equifax conduct regular database scanning and securing checks;

g. Ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Equifax to meaningfully educate consumers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps consumers should take to protect themselves.

200.

Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Georgia Plaintiffs and Georgia Class Members and the public from Equifax's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Equifax's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

201.

Plaintiffs' GFBPA claims are appropriate for class certification in federal court. *See Shady Grove Orthopedic Assoc. PA v. Allstate Ins. Co.*, 559 U.S. 393 (2010); *Lisk v. Lumber One Wood Preserving, LLC*, 792 F.3d 1331 (11th Cir. 2015).

202.

Georgia Plaintiffs and Georgia Class Members are entitled to a judgment against Equifax for actual and consequential damages, exemplary damages and attorneys' fees pursuant to the GFBPA, costs, and such other further relief as the Court deems just and proper.

COUNT VIII- VIOLATION OF FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT ("FDUPTPA") FLA. STA. § 501.201, ET SEQ. (ON BEHALF OF FLORIDA PLAINTIFF AND THE FLORIDA CLASS)

203.

Florida Plaintiff Moore realleges, as if fully set forth, the allegations of paragraphs Nos. 1-202 above.

204.

Equifax is engaged in, and their acts and omissions affect, trade and commerce pursuant to Fla. Sta. § 501.201 of FDUTPA.

205.

Plaintiff Moore and Florida Class Members entrusted Equifax with their PII.

206.

As alleged herein this Complaint, Equifax engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the FDUTPA:

a. failure to maintain adequate computer systems and data security practices to safeguard PII;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to timely and accurately disclose the Data Breach to Plaintiff Moore and Florida Class Members;

d. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the Data Breach and before it allegedly remediated the Breach.

207.

Furthermore, as alleged above, Equifax's failure to secure consumers' PII violates the FTCA and therefore violates the FDUTPA.

208.

Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff Moore and

Florida Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

209.

As a direct and proximate result of Equifax's violation of the FDUTPA, Plaintiff Moore and Florida Class Members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff Moore and Florida Class Members; damages arising from Plaintiff Moore's and Florida Class Members' inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards and damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching,

adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

210.

Also as a direct result of Equifax's knowing violation of the FDUTPA, Plaintiff Moore and Florida Class Members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Equifax segment PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. Ordering that Equifax purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Equifax conduct regular database scanning and securing checks;

g. Ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Equifax to meaningfully educate consumers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps consumers should take to protect themselves.

211.

Plaintiff Moore brings this action on behalf of himself and Florida Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow

consumers to make informed purchasing decisions and to protect Plaintiff Moore and Florida Class Members and the public from Equifax's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Equifax's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

212.

Plaintiff Moore and Florida Class Members are entitled to a judgment against Equifax for actual and consequential damages, exemplary damages and attorneys' fees pursuant to the FDUTPA, costs, and such other further relief as the Court deems just and proper.

COUNT IX- VIOLATION OF SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT ("UTPA") S.C. CODE ANN. § 39-5-10 TO-160 (1991), ET SEQ. (ON BEHALF OF SOUTH CAROLINA PLAINTIFFS AND THE SOUTH CAROLINA CLASS)

213.

South Carolina Plaintiffs reallege, as if fully set forth, the allegations of paragraphs Nos. 1-212 above.

214.

Equifax is engaged in, and their acts and omissions affect, trade and commerce pursuant to S.C. Code Ann. § 39-5-10 to-160 (1991) of UTPA.

215.

South Carolina Plaintiffs and South Carolina Class Members entrusted Equifax with their PII.

216.

As alleged herein this Complaint, Equifax engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the UTPA:

a. failure to maintain adequate computer systems and data security practices to safeguard PII;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to timely and accurately disclose the Data Breach to South Carolina Plaintiffs and South Carolina Class Members;

d. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the Data Breach and before it allegedly remediated the Breach.

217.

Furthermore, as alleged above, Equifax's failure to secure consumers' PII violates the FTCA and therefore violates the UTPA.

218.

Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of South Carolina Plaintiffs and South Carolina Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

219.

As a direct and proximate result of Equifax's violation of the UTPA, South Carolina Plaintiffs and South Carolina Class Members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiffs and Class Members; damages arising from Plaintiffs' inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards and damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes"

and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

220.

Also as a direct result of Equifax's knowing violation of the UTPA, South Carolina Plaintiffs and South Carolina Class Members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Equifax segment PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. Ordering that Equifax purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Equifax conduct regular database scanning and securing checks;

g. Ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Equifax to meaningfully educate consumers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps consumers should take to protect themselves.

221.

Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect South Carolina Plaintiffs and South Carolina Class Members and the public from Equifax's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Equifax's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

222.

South Carolina Plaintiffs and South Carolina Class Members are entitled to a judgment against Equifax for actual and consequential damages, exemplary damages and attorneys' fees pursuant to the UTPA, costs, and such other further relief as the Court deems just and proper.

COUNT X- VIOLATION OF SOUTH CAROLINA DATA BREACH ACT S.C. CODE ANN. § 39-1-90 (2012), ET SEQ. (ON BEHALF OF SOUTH CAROLINA PLAINTIFFS AND THE SOUTH CAROLINA CLASS)

223.

Plaintiffs reallege, as if fully set forth, the allegations of paragraphs Nos. 1-222 above.

224.

Equifax conducted business in South Carolina and at all relevant times, owned and possessed PII of South Carolina Plaintiffs and South Carolina Class Members.

225.

The Data Breach constituted a security breach that triggered the notice provisions, Section 39-1-90(a) of the South Carolina Data Breach Act and the PII taken includes categories of PII protected by the South Carolina Data Breach Act.

226.

Equifax unreasonably delayed in informing South Carolina Plaintiffs and South Carolina Class Members about the Data Breach after Equifax knew or should have known that the Data Breach had occurred.

227.

South Carolina Plaintiffs and South Carolina Class Members were damaged and harmed by Equifax's failure to comply with the South Carolina Data Breach Act.

228.

Equifax violated the South Carolina Data Breach Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards.

229.

Equifax's violation of the South Carolina Data Breach Act constitutes negligence per se.

230.

South Carolina Plaintiffs and South Carolina Class Members are within the class of persons that the South Carolina Data Breach Act was intended to protect.

231.

The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to safeguard against.

232.

Had Equifax provided timely and accurate notice, South Carolina Plaintiffs and South Carolina Class Members could have avoided or mitigated the harm caused by the Data Breach. For example, they could have contacted their banks

to cancel any affected cards or taken security precautions in time to prevent or minimize identity theft.

233.

Plaintiffs and Class Members seek all remedies available under S.C. Code Ann. § 39-1-90 (2012), including but not limited to damages, equitable relief, including injunctive relief, treble damages, reasonable attorneys' fees and costs, as provided by the applicable laws.

COUNT XI- VIOLATION OF TENNESSEE CONSUMER PROTECTION ACT ("TCPA") TENN. CODE ANN. § 47-18-104, ET SEQ. (ON BEHALF OF TENNESSEE PLAINTIFF AND THE TENNESSEE CLASS)

234.

Tennessee Plaintiff Williams realleges, as if fully set forth, the allegations of paragraphs Nos. 1-233 above.

235.

Equifax is engaged in, and their acts and omissions affect, trade and commerce pursuant to Tenn. Code Ann. § 47-18-104(a), (b)(2), (3), and (7) of TCPA.

236.

Plaintiff Williams and Tennessee Class Members entrusted Equifax with their PII.

237.

As alleged herein this Complaint, Equifax engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the TCPA:

a. failure to maintain adequate computer systems and data security practices to safeguard PII;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to timely and accurately disclose the Data Breach to Plaintiff Williams and Tennessee Class Members;

d. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

e. continued acceptance of PII and storage of other personal information after Equifax knew or should have known of the Data Breach and before it allegedly remediated the Breach.

238.

Furthermore, as alleged above, Equifax's failure to secure consumers' PII violates the FTCA and therefore violates the TCPA.

239.

Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff Williams and Tennessee Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

240.

As a direct and proximate result of Equifax's violation of the TCPA, Plaintiff Williams and Tennessee Class Members suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiffs and Class Members; damages arising from Plaintiffs' inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards and damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their

credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

241.

Also as a direct result of Equifax's knowing violation of the TCPA, Plaintiff Williams and Tennessee Class Members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Equifax segment PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. Ordering that Equifax purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Equifax conduct regular database scanning and securing checks;

g. Ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Equifax to meaningfully educate consumers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps consumers should take to protect themselves.

242.

Plaintiffs bring this action on behalf of themselves and Class Members for

the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff Williams and Tennessee Class Members and the public from Equifax's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Equifax's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

243.

Plaintiff Williams and Tennessee Class Members are entitled to a judgment against Equifax for actual and consequential damages, exemplary damages and attorneys' fees pursuant to the TCPA, costs, and such other further relief as the Court deems just and proper.

COUNT XII- VIOLATION OF TENNESSEE DATA BREACH ACT, TENN. CODE ANN. § 47-18-2107(b), *ET SEQ.*; (ON BEHALF OF TENNESSEE PLAINTIFF AND THE TENNESSEE CLASS)

244.

Tennessee Plaintiff Williams realleges, as if fully set forth, the allegations of paragraphs Nos. 1-243 above.

245.

Equifax conducted business in Tennessee and at all relevant times, owned and possessed PII of Plaintiff Williams and Tennessee Class Members.

246.

The Data Breach constituted a security breach that triggered the notice provisions, § 47-18-2107(b) of the Tennessee Data Breach Act and the PII taken includes categories of PII protected by the Tennessee Data Breach Act.

247.

Equifax unreasonably delayed in informing Plaintiff Williams and Tennessee Class Members about the Data Breach after Equifax knew or should have known that the Data Breach had occurred.

248.

Plaintiff Williams and Tennessee Class Members were damaged and harmed by Equifax's failure to comply with the Tennessee Data Breach Act.

249.

Plaintiff Williams and Tennessee Class Members were damaged and harmed by Equifax's failure to comply with the Tennessee Data Breach Act.

250.

Equifax violated the Tennessee Data Breach Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards.

251.

Equifax's violation of the Tennessee Data Breach Act constitutes negligence per se.

252.

Plaintiff Williams and Tennessee Class Members are within the class of persons that the Tennessee Data Breach Act was intended to protect.

253.

Had Equifax provided timely and accurate notice, Plaintiff Williams and Tennessee Class Members could have avoided or mitigated the harm caused by the Data Breach. For example, they could have contacted their banks to cancel any affected cards or taken security precautions in time to prevent or minimize identity theft.

254.

Plaintiff Williams and Tennessee Class Members seek all remedies available under Tenn. Code Ann. § 47-18-2107(b), including but not limited to

damages, equitable relief, including injunctive relief, treble damages, reasonable attorneys' fees and costs, as provided by the applicable laws.

COUNT XIII- UNJUST ENRICHMENT (ON BEHALF OF PLAINTIFFS AND THE NATIONAL, GEORGIA, FLORIDA, SOUTH CAROLINA, AND TENNESSEE CLASSES)

255.

Plaintiffs reallege, as if fully set forth, the allegations of paragraphs Nos. 1-254 above.

256.

Plaintiffs and Class Members conferred a monetary benefit on Equifax. Specifically, they purchased products and services from Equifax at retail prices and provided Equifax with their PII by using their credit or debit cards for the purchases. In exchange, Plaintiffs and Class Members should have been compensated by Equifax with the products or services that were the subject of the transaction and by having Equifax process and store their PII using adequate data security.

257.

Plaintiff Nancy Vita, for example, purchased Equifax's monitoring software during the time period in which Equifax knew or should have known about the Data Breach. Equifax, thus, knew or should have known that her PII

was or would be compromised. Had Ms. Vita known about the Data Breach, she would not have purchased the monitoring software. Equifax failed to inform Ms. Vita of the Data Breach at the time of the transaction.

258.

Equifax knew that Plaintiffs and Class Members conferred a benefit on Equifax. Equifax profited from their purchases and used their PII for its own business purposes.

259.

Equifax failed to secure the Plaintiffs' and Class Members' PII, and, therefore, did not provide full compensation for the benefit the Plaintiffs and Class Members provided.

260.

Equifax acquired the PII through inequitable means because it failed to disclose the inadequate security practices previously alleged.

261.

Had Plaintiffs and Class Members known that Equifax would not secure their PII using adequate security, they would not have completed their purchases with Equifax.

262.

Plaintiffs and Class Members have not adequate remedy at law.

263.

Under the circumstances, it would be unjust for Equifax to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred on it.

264.

Equifax should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and Class Members proceeds that it unjustly received from them. In the alternative, Equifax should be compelled to refund the amounts that Plaintiffs and Class Members overpaid.

COUNT XIV BAILMENT (ON BEHALF OF PLAINTIFFS AND THE NATIONAL, GEORGIA, FLORIDA, SOUTH CAROLINA, AND TENNESSEE CLASSES)

265.

Plaintiffs reallege, as if fully set forth, the allegations of paragraphs Nos. 1-264 above.

266.

Plaintiffs and the other Class Members entrusted their PII to Equifax for credit related services. Plaintiffs and other Class Members were entitled to trust

that their PII in Equifax's possession would likewise be properly protected from unlawful access whether or not they originally entrusted it to Equifax.

267.

Plaintiffs' and the other Class Members' PII is their personal property. Equifax's wrongful actions and/or inaction and the resulting data breach deprived them of the value of their PII, for which there is a well-established national and international market, because the PII is now in the hands of unauthorized person(s) and compromised.

COUNT XV- DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF (ON BEHALF OF PLAINTIFFS AND THE NATIONAL, GEORGIA, FLORIDA, SOUTH CAROLINA, AND TENNESSEE CLASSES)

268.

Plaintiffs reallege, as if fully set forth, the allegations of paragraphs Nos. 1-267 above.

269.

As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Equifax to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Equifax

owes duties of care to Plaintiffs and Class Members that require it to adequately secure PII.

270.

Equifax still possesses PII pertaining to Plaintiffs and Class Members.

271.

Equifax has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

272.

Accordingly, Equifax has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Equifax's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

273.

Actual harm has arisen in the wake of the Equifax Data Breach regarding Equifax's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class Members.

274.

Plaintiffs, therefore, seek a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually 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; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

275.

Plaintiffs seek injunctive relief, including indefinite, continuing credit monitoring for victims of the Data Breach, as well as insurance for victims to cover identity theft and the damages flowing therefrom.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Equifax as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs and their Counsel to represent the National Class, or in the alternative the separate Statewide Classes;

b. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class Members;

c. For equitable relief compelling Equifax to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class Members the type of PII compromised;

d. For an award of damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demands a jury trial on all issues so triable.

THIS IS TO CERTIFY that, pursuant to LR 5.1B, N.D. Ga., the above document was prepared in Times New Roman, 14 pt.

This 11th day of September, 2017

HALL & LAMPROS, LLP

/s/Christopher B. Hall
Christopher B. Hall
Ga. Bar No. 318380
Andrew Lampros
Ga. Bar No. 432328

Promenade II
1230 Peachtree Street, NE
Atlanta, GA 30309
Tel: (404) 876-8100
Fax: (404-876-3477
chall@hallandlampros.com
alampros@hallandlampros.com

PRATT CLAY, LLC
Bradley Pratt
Ga Bar No. 586672
Charles L. Clay, Jr.
Ga Bar No. 129505
Brian C. Mickelsen
Ga Bar No. 30307

4401 Northside Parkway, NW
Suite 520

Atlanta, GA 30327
Tel: (404) 949-8118
bradley@prattclay.com
chuck@prattclay.com
brian@prattclay.com

Counsel for Plaintiffs and the Proposed Class

JS44 (Rev. 6/2017 NDGA)

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)

NANCY M. VITA, HORACE C. RAMEY, JAMES A. BLACK, JIMMIE MOORE,THOMAS A. WILLIAMS, DANIEL R. DALTON, BRITTANY S. DALTON, Georgia consumers, Florida consumers, Tennessee consumers, South Carolina consumers, individually and on behalf of all others,

DEFENDANT(S)

EQUIFAX, INC.

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF COBB COUNTY, GA
(EXCEPT IN U.S. PLAINTIFF CASES)

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)

HALL & LAMPROS, LLP
1230 Peachtree St. NE, Suite 950
Atlanta, Georgia 30309
(404) 876-8100
chall@hallandlampros.com
alampros@hallandlampros.com

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION

(PLACE AN "X" IN ONE BOX ONLY)

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

III. CITIZENSHIP OF PRINCIPAL PARTIES

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

PLF	DEF		PLF	DEF	
☐ 1	☑ 1	CITIZEN OF THIS STATE	☐ 4	☑ 4	INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
☑ 2	☐ 2	CITIZEN OF ANOTHER STATE	☐ 5	☐ 5	INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
☐ 3	☐ 3	CITIZEN OR SUBJECT OF A FOREIGN COUNTRY	☐ 6	☐ 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 § 1332(d)(2)
Consumer Data Breach

(IF COMPLEX, CHECK REASON BELOW)

- ☑ 1. Unusually large number of parties.
- ☑ 2. Unusually large number of claims or defenses.
- ☑ 3. Factual issues are exceptionally complex
- ☐ 4. Greater than normal volume of evidence.
- ☐ 5. Extended discovery period is needed.
- ☐ 6. Problems locating or preserving evidence
- ☐ 7. Pending parallel investigations or actions by government.
- ☐ 8. Multiple use of experts.
- ☐ 9. Need for discovery outside United States boundaries.
- ☐ 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 _____ NATURE OF SUIT _____ CAUSE OF ACTION _____
(Referral)

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 (ANDA) - 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 ANTITRUST
- ☐ 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 $**_____

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

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE William S. Duffy, Jr. **DOCKET NO.** 1:17-cv-03422-WSD

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/ Christopher B. Hall 09/11/2017

SIGNATURE OF ATTORNEY OF RECORD **DATE**