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

RANDOLPH JEFFERSON CARY III, WILLIAM R. PORTER, and ROBIN D. PORTER, individually, and on behalf of all others similarly situated,	)	Case No.
Plaintiffs,	)	
v.	)	
EQUIFAX, INC.,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiffs Randolph Jefferson Cary III, William R. Porter, and Robin D. Porter ("Plaintiffs"), on behalf of themselves and all others similarly situated, allege upon personal knowledge as to themselves, and upon information and belief, including the investigation of counsel, as follows:

NATURE OF ACTION

1. On September 7, 2017, Equifax announced a nationwide data breach affecting an estimated 143 million Americans (the "Data Breach"). According to Equifax's statement, unauthorized parties accessed consumers' sensitive, personal information was exploited through a "website application vulnerability" on

Equifax's servers. The information included names, birth dates, Social Security numbers, addresses and some driver's license numbers, 209,000 U.S. credit card numbers, and "certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers" (collectively "Personal Information").

2. The Data Breach occurred because Equifax failed to implement adequate security measures to safeguard consumers' Personal Information and willfully ignored known weaknesses in its data security, including prior hacks into its information systems. Unauthorized parties routinely attempt to gain access to and steal personal information from networks and information systems—especially from entities such as Equifax, which are known to possess a large number of individuals' valuable personal and financial information.

3. As a result of Equifax's willful failure to prevent the breach, Plaintiffs and Class members have been exposed to fraud, identity theft, and financial harm, as detailed below, and to a heightened, imminent risk of such harm in the future. Plaintiff and Class members have to monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur, additional out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures in order to detect, protect, and repair the Data Breach's

impact on their Personal Information for the remainder of their lives. Plaintiffs and Class members anticipate spending considerable time and money for the rest of their lives in order to detect and respond to the impact of the Data Breach.

4. Plaintiffs bring this action to remedy these harms on behalf of themselves and all similarly situated individuals whose Personal Information was compromised in the Data Breach. Plaintiffs seek the following remedies, among others: statutory damages under the Fair Credit Reporting Act ("FCRA") and state consumer protection statutes, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance beyond Equifax's one-year current offer, and injunctive relief including an order requiring Equifax to implement improved data security measures.

PARTIES

5. Plaintiff Randolph Jefferson Cary III is a resident and citizen of Atlanta, Georgia and had his Personal Information compromised in the Data Breach.

6. Plaintiffs William R. Porter and Robin D. Porter are residents and citizens of Osteen, Florida and had their Personal Information compromised in the Data Breach.

7. Defendant Equifax, Inc. ("Equifax") is a Georgia limited liability company authorized to do business throughout the United States. Equifax is a "consumer reporting agency" as defined in 15 U.S.C. § 1681a(f). Equifax, Inc. may be served through its registered agent, Shawn Baldwin, at its principal office located at 1550 Peachtree Street NE, Atlanta, Georgia 30309.

JURISDICTION AND VENUE

8. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) ("The Class Action Fairness Act") because sufficient diversity of citizenship exists between parties in this action, the aggregate amount in controversy exceeds $5,000,000, and there are 100 or more members of the Class.

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

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) 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.

FACTUAL ALLEGATIONS

The Data Breach

11. Equifax is a credit reporting agency that collects information about where consumers live, work, make payments on their credit accounts, as well as their arrest, lawsuit, and bankruptcy histories. Equifax then combines this information together in a credit report, which is compiled for the purpose of selling it to creditors, employers, insurers, and others who may want to access the information. These companies will use the credit reports to make decisions about extending credit, jobs, and insurance policies, and for other purposes.

12. On September 7, 2017, Equifax announced that it has been subject to one of the largest data breaches in U.S. history impacting 143 million U.S. consumers, or nearly half the U.S. population.

13. Equifax stated in a press release that the "information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with

personal identifying information for approximately 182,000 U.S. consumers, were accessed."

14. Equifax acknowledged it discovered the breach on July 29, 2017, and then engaged a cybersecurity firm to conduct a "comprehensive forensic review." The investigation concluded that the unauthorized access occurred from mid-May through July 2017.

15. Unlike other data breaches, the Data Breach did not just affect customers of Equifax, but also millions of individuals who have never voluntarily provided their information to Equifax. Indeed, in its role as a credit reporting agency, Equifax gathers and maintains information on over 800 million consumers and more than 88 million businesses worldwide. Equifax's revenue in 2016, derived primarily from selling access to consumers' credit reports, was over $3 billion.

16. Equifax is well aware that securing the personal information it gathers is central to the lifeblood of its business. Equifax CEO and Chairman Richard Smith acknowledged as much in his statement about the breach: "This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes. We pride ourselves on being a leader in

managing and protecting data, and we are conducting a thorough review of our overall security operations."

17. While Equifax said attackers were able to break into the company's systems by exploiting an application vulnerability to gain access to certain files, it did not say which application or which vulnerability was the source of the breach. Cybersecurity blogger Brian Krebs speculated: "It's unclear why Web applications tied to so much sensitive consumer data were left unpatched, but a lack of security leadership at Equifax may have been a contributing factor. Until very recently, the company was searching for someone to fill the role of vice president of cybersecurity, which according to Equifax is akin to the role of a chief information security officer (CISO)."[1]

18. Equifax was a known and obvious target. As noted by the *New York Times*, Equifax "is a particularly tempting target for hackers. If identity thieves wanted to hit one place to grab all the data needed to do the most damage, they would go straight to one of the three major credit reporting agencies."[2]

---

[1] Brian Krebs, *Breach at Equifax May Impact 143M Americans*, KREBS ON SECURITY, (September 7, 2017), https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/ (last visited September 8, 2017).

[2] Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber, *Equifax Says Cyberattack May Have Affected 143 Million Customers*, NEW YORK TIMES, (September 7, 2017) https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?mcubz=0 (last visited September 8, 2017).

19. Experts agree that the Data Breach has the potential to be one of the most damaging in history. John Ulzheimer, a credit expert who previously worked at FICO and Equifax, said cybercriminals have now accessed the "crown jewels of information" at Equifax.[3] Pamela Dixon, executive director of the World Privacy Forum, a nonprofit research group, said that: "This is about as bad as it gets. If you have a credit report, chances are you may be in this breach. The chances are much better than 50 percent."[4] Avivah Litan, a fraud analyst at Gartner, stated that: "On a scale of 1 to 10 in terms of risk to consumers, this is a 10."[5]

20. Ironically, Equifax's notice to consumers includes a section entitled "Identity Theft Prevention Tips" that warns customers to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports" and encourages them to do so by *purchasing their credit report from Equifax*, among others. Equifax also offered consumers one year of credit monitoring services through a company *owned and operated by Equifax*.

---

[3] Katie Lobosco, *How to find out if you're affected by the Equifax hack*, CNN MONEY, (September 7, 2017), https://amp.cnn.com/money/2017/09/07/pf/victim-equifax-hack-how-to-find-out/index.html (last visited September 8, 2017).

[4] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?mcubz=0.

[5] *Id.*

Equifax Holds Itself as "The Leading Provider of Data Breach Services" and Promised to Protect Consumers' Personal Information, but Maintained Inadequate Data Security.

21. Equifax is one of the three major credit reporting agencies in the United States. As a credit reporting agency, Equifax is engaged in a number of credit-related services and holds itself out as "a consumer advocate, steward of financial literacy, and champion of economic advancement" and "an innovative global information solutions company that enables access to credit."[6]

22. Prior to the Data Breach, Equifax promised its customers and everyone else whose Personal Information it collects that it would reasonably protect their Personal Information. Equifax's privacy policy stated, in relevant part, that: "For more than 100 years, Equifax has been a catalyst for commerce by bringing businesses and consumers together. Equifax also provides products and services that bring businesses together with other businesses. We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information

[6] http://www.equifax.com/about-equifax/.

we have about businesses. ***Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax***."[7]

23. Equifax maintains multiple "privacy policies" that purport to apply to different sects of its customers or consumers. For example, Equifax's privacy policy related to "Activities by Consumers Related to Credit Reports" states that:

> **Information Collection and Use**
> We collect personal and non-personal information on our web site to fulfill your requests and contact you.
>
> There are aspects of our site that can be enjoyed as a visitor, but you need to provide us with personal information in order to perform Consumer Activities associated with your credit file, such as requesting an annual disclosure of your credit file, disputing of information in your credit file, or placing a security freeze or an initial fraud alert.
>
> **Information We Collect From You**
> **Contacting Equifax with a request:** We receive information from you when you perform one of the Consumer Activities through our site. We also receive information from you when you register for an Equifax Personal Solutions account in order to maintain online access to your free annual credit file disclosure for 30 days. This information may include:
>
> - First and last name (middle initial and suffix, as applicable);
> - Social Security number;
> - Date of birth;
> - Home telephone number;
> - E-mail address;
> - Current and former mailing address; and
> - Credit card number and expiration date.

[7] http://www.equifax.com/privacy/.

***

Log information: When you visit our site, our servers automatically collect log information. This information may include your web page request, Internet Protocol (IP) address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser. We collect log information so that we can properly administer our system and gather aggregate information about how our site is being used, including the pages visitors are viewing on our site.

***

Information We Collect From Others

We also collect information about you from third parties, including AnnualCreditReport.com (the centralized service for consumers to request their free annual credit reports), parties from whom we request information in connection with your request for dispute resolution, the centralized pre-screening opt-out management service, and other credit reporting agencies when you place initial fraud or active duty alerts.

When we associate information that we obtain from third parties with personal information that we have collected under this policy, we will treat the acquired information like the information that we collected ourselves. We will not share information we obtain from third parties in personally identifiable form. However, we may share aggregated, non-personal information as described in this policy, including information we obtained from third parties, in a form that will not allow you to be identified.

How We Use Collected Information

We use the information we collect about you to administer our web site, improve the user experience, and provide you with the information or services you request.

In connection with your one or more Consumer Activities, we will use your email address to communicate with you regarding the status of your online request.

> **To Whom We May Disclose the Information We Collect**
> We take reasonable precautions to be sure that nonaffiliated third parties and affiliates to whom we disclose your personally identifiable information are aware of our privacy policy and will treat the information in a similarly responsible manner. Our contracts and written agreements with nonaffiliated third parties that receive information from us about you prevent further transfer of the information.
>
> We will ***not disclose*** your personal information to third parties except to provide you with the disclosure or service you request, or under certain circumstances as described in this policy.[8]

24. By permitting unauthorized access to consumers' Personal Information, Equifax failed to comply with its own privacy policy.

25. There is no question Equifax recognizes the risks of a data breach because it markets and sells "data breach solutions" to consumers and businesses. In its marketing materials, Equifax states: "You'll feel safer with Equifax. We're the leading provider of data breach services, serving more than 500 organizations with security breach events everyday. In addition to extensive experience, Equifax has the most comprehensive set of identity theft products and customer service coverage in the market."[9]

Equifax Has a History of Lax Data Security Practices

[8] http://www.equifax.com/privacy/personal-credit-reports (emphasis added).

[9] http://www.equifax.com/help/data-breach-solutions/.

26. Equifax has a history of major data security blunders. In 2010, tax forms mailed by Equifax's payroll vendor had Equifax employees' SSNs partially or fully viewable through the envelope's return address window. One affected Equifax employee stated "If they can't do this internally how are they going to be able to go to American Express and other companies and say we can mitigate your liability? They are first-hand delivering information for the fraudsters out there. It's so terribly sad. It's just unacceptable, especially from a credit bureau."[10]

27. In March 2013, Equifax confirmed "fraudulent and unauthorized" access to the credit reports of multiple celebrities and top Washington, D.C. officials, including First Lady Michelle Obama and Vice President Joe Biden.[11]

28. In March 2015, Equifax notified certain consumers that personal information contained on their credit file was erroneously sent to unauthorized individuals due to a technical error during a software change.[12]

---

[10] Elinor Mills, *Equifax tax forms expose worker Social Security numbers*, CNET, (Feb. 11, 2010), http://www.cnet.com/news/equifax-tax-forms-expose-worker-social-security-numbers/ (last visited September 8, 2017).

[11] *U.S. probes hack of credit data on Mrs Obama, Beyonce, others*, REUTERS, (March 12, 2013), http://www.reuters.com/article/us-usa-cybersecurity-hacking-idUSBRE92B12520130313 (last visited September 8, 2017).

[12] *Data Incident Notification to New Hampshire Attorney General*, (April 2, 2015), http://doj.nh.gov/consumer/security-breaches/documents/equifax-20150402.pdf (last visited September 8, 2017).

29. Also in March 2015, Equifax mistakenly sent a Maine woman the full credit reports of more than 300 other individuals, which exposed their SSNs, dates of birth, current and previous addresses, creditor information, and bank and loan account numbers, among other sensitive information. The woman told reporters "I'm not supposed to have this information, this is unbelievable, someone has messed up."[13]

30. In May 2016, it was discovered that a product offered by Equifax's subsidiary company Equifax Workforce Solutions, Inc. (d/b/a TALX), a purveyor of products and services related to Human Resources, payroll, and tax management and compliance, contained a major security vulnerability that affected employees at grocery giant Kroger and others.

31. As noted at the time by Krebs, "Equifax's W-2Express site makes electronic W-2 forms accessible for download for many companies, including Kroger — which employs more than 431,000 people. According to a letter Kroger sent to employees dated May 5, thieves were able to access W-2 data merely by entering at Equifax's portal the employee's default PIN code, which was nothing

[13] Jon Chrisos, *Credit agency mistakenly sends 300 confidential reports to Maine woman*, BANGOR DAILY NEWS, (March 19, 2015), http://bangordailynews.com/2015/03/19/news/state/credit-agency-mistakenly-sends-300-confidential-reports-to-maine-woman/ (last visited September 8, 2017).

more than the last four digits of the employee's Social Security number and their four-digit birth year."[14]

32. Krebs reported that in 2016 Equifax suffered at least three data breaches relating to its W-2 database alone. While Kroger was the largest, Krebs reported that earlier in the year, employees at Stanford University and Northwestern University also had their information breached via the W-2Express portal.[15]

Equifax's Response to the Data Breach was Haphazard and Untimely

33. Despite learning of the Data Breach on July 29, 2017, Equifax failed to timely and accurately notify customers of the Data Breach in the most expedient time possible and without unreasonable delay, instead waiting over a month to inform the general public. During that time affected individuals could have taken precautions like placing security freezes on their credit in order to prevent or detect fraudulent activity.

[14] Brian Krebs, Crooks Grab W-2s from Credit Bureau Equifax, KREBS ON SECURITY, (May 6, 2016), https://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/ (last visited September 8, 2017).

[15] *Id.*

34. Making matters worse, Bloomberg reported that three Equifax senior executives sold shares worth almost $1.8 million in the days after the company discovered a security breach, but long before it was announced publicly.[16]

35. Along with its press release, Equifax directed consumers to a website it created regarding the breach, https://www.equifaxsecurity2017.com. The website purported to allow consumers to look up whether they were affected by the breach by inputting their last name and the last-6 numbers of their Social Security number, as well as enroll in one year of TrustedID Premier, a credit monitoring service that is ***owned and operated by Equifax***.

36. Almost immediately after its announcement, Equifax's website started malfunctioning. As summarized by Krebs, "[a]t time of publication, the Trustedid.com site Equifax is promoting for free credit monitoring services was only intermittently available, likely because of the high volume of traffic following today's announcement. As many readers here have shared in the comments already, the site Equifax has available for people to see whether they were impacted by the breach may not actually tell you whether you were affected. When

[16] Anders Melin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed*, Bloomberg, (September 7, 2017), https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack (last visited September 8, 2017).

I entered the last six digits of my SSN and my last name, the site threw a "system unavailable" page, asking me to try again later."[17]

37. Later in the day, consumers received a vague message that they could enroll in credit monitoring on a specified later date, but it did not specifically state whether they were impacted, as Equifax told consumers it would. As noted by Krebs, "Maybe Equifax simply isn't ready to handle everyone in America asking for credit protection all at once, but this could be seen as a ploy by the company assuming that many people simply won't return again after news of the breach slips off of the front page. At a reader's suggestion, I used a made-up last name and the last six digits of my Social Security number: The system returned the same response: Come back on Sept. 13. It's difficult to tell if the site is just broken or if there is something more sinister going on here."[18]

38. Krebs also highlighted another common complaint related to the credit monitoring services offered by Equifax: "The fact that the breached entity (Equifax) is offering to sign consumers up for its own identity protection services strikes me as pretty rich. Typically, the way these arrangements work is the credit

[17] Brian Krebs, *Breach at Equifax May Impact 143M Americans*, Krebs On Security, (September 7, 2017), https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/ (last visited September 8, 2017).

[18] *Id.*

monitoring is free for a period of time, and then consumers are pitched on purchasing additional protection when their free coverage expires. In the case of this offering, consumers are eligible for the free service for one year."[19]

39. In other words, Equifax is offering access to a product that it has the ability to profit from down the road, and also requires consumers to provide more of their Personal Information to Equifax.

40. Lawmakers are also criticizing Equifax. In a statement, Sen. Mark Warner (D-Va.), who heads the bipartisan Senate Cybersecurity Caucus, called the Equifax breach "profoundly troubling" and noted: "While many have perhaps become accustomed to hearing of a new data breach every few weeks, the scope of this breach – involving Social Security Numbers, birth dates, addresses, and credit card numbers of nearly half the U.S. population – raises serious questions about whether Congress should not only create a uniform data breach notification standard, but also whether Congress needs to rethink data protection policies, so that enterprises such as Equifax have fewer incentives to collect large, centralized sets of highly sensitive data like SSNs and credit card information on millions of Americans. It is no exaggeration to suggest that a breach such as this – exposing highly sensitive personal and financial information central for identity management

[19] *Id.*

and access to credit – represents a real threat to the economic security of Americans."

The Effect of the Data Breach on Plaintiffs and the Class

41. The ramifications of Equifax's failure to protect the sensitive personal and tax information of its clients' employees are severe. Identity thieves can use the information stolen in the Data Breach to perpetrate a wide variety of crimes, including tax fraud, identity theft such as opening fraudulent credit cards and loan accounts, as well as various types of government fraud such as changing immigration status using the victim's name, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, obtaining a job, procuring housing, or even giving false information to police during an arrest. In the medical context, consumers' stolen Personal Information can be used to submit false insurance claims, obtain prescription drugs or medical devices for black-market resale, or get medical treatment in the victim's name.

42. The U.S. Social Security Administration (SSA) warns that "[i]dentity theft is one of the fastest growing crimes in America."[20] The SSA has stated that

[20] *Identity Theft And Your Social Security Number, Social Security Administration* (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited September 8, 2017).

"[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought." In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[21]

43. Under SSA policy, individuals cannot obtain a new Social Security number until there is evidence of ongoing problems due to misuse of the Social Security number. Even then, the SSA recognizes that "a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start."[22]

[21] *Id.*

[22] *Id.*

44. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[23]

45. The processes of discovering and dealing with the repercussions of identity theft are time consuming and difficult. The Department of Justice's Bureau of Justice statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[24] Likewise, credit monitoring services are reactive not preventative, meaning they cannot catch identity theft until after it happens.

46. Additionally, there is commonly lag time between when harm occurs and when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "law enforcement officials told

[23] *Id*.

[24] Erika Harrell and Lynn Langton, *Victims of Identity Theft, 2012*, (Bureau of Justice Statistics), Dec. 2013, http://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited September 8, 2017).

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. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[25]

47. There is a very strong probability that Equifax victims are at imminent risk of further fraud and identity theft for years into the future. As a result of Equifax's negligent security practices and delay in notifying affected individuals, Plaintiffs and other Class members now face years of constant monitoring of their financial and personal accounts and records to account for identity theft and fraud. Plaintiffs and Class members be faced with fraudulent debt, or incur costs for, among other things, paying monthly or annual fees for identity theft and credit monitoring services, obtaining credit reports, credit freezes, and other protective measures to deter, detect, and mitigate the risk of identity theft and fraud.

[25] U.S. Government Accountability Office, GAO Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, http://www.gao.gov/new.items/d07737.pdf (last visited September 8, 2017).

48. As a result of the compromising of their Personal Information, Plaintiffs and Class members have or may suffer one or a combination of the following injuries:

a. incidents of identity fraud and theft, including unauthorized bank activity,

b. fraudulent credit card purchases, and damage to their credit;

c. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of Personal Information;

d. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach, including but not limited to efforts to research how to prevent, detect, contest, and recover from misuse of their Personal Information; and

e. loss of the opportunity to control how their Personal Information is used.

49. Furthermore, Plaintiffs and Class members have suffered, and/or will face an increased risk of suffering in the future, the following injuries:

a. money and time lost as a result of fraudulent access to and use of

their financial accounts;

b. loss of use of and access to their financial accounts and/or credit;

c. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

d. lowered credit scores resulting from credit inquiries following fraudulent activities;

e. costs and lost time obtaining credit reports in order to monitor their credit records;

f. money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;

g. money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;

h. costs of credit monitoring that is more robust than the services being offered by Equifax;

i. anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;

j. costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling

compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

k. money and time expended to ameliorate the consequences of the filing of fraudulent tax returns; and

l. continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Equifax fails to undertake appropriate, legally required steps to protect the personal information in its possession.

CLASS ACTION ALLEGATIONS

50. Plaintiffs bring this action on behalf of themselves and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and/or (c)(4), seeking damages and equitable relief on behalf of the following class:

> All persons residing in the United States whose Personal Information was compromised in the data breach announced by Equifax in September 2017 (the "Nationwide Class").

51. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims under the laws of the individual States, and on behalf of separate statewide classes, defined as follows:

> All persons residing in [STATE] whose Personal Information was compromised in the data breach announced by Equifax in September 2017 (the "Statewide Classes").

52. Excluded from the Class are: Equifax; its parent companies, subsidiaries and affiliates; federal governmental entities and instrumentalities of the federal government; and states and their subdivisions, agencies and instrumentalities.

53. **Numerosity. Fed. R. Civ. P. 23(a)(1)**. Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, the proposed Class include at least 143 million individuals whose Personal Information was compromised in the Equifax Data Breach. 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.

54. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3)**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Equifax had a duty to protect Personal Information;

b. Whether Equifax knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether Equifax's security measures to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Equifax was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Equifax's failure to implement adequate data security measures allowed the breach to occur;

f. Whether Equifax's conduct constituted deceptive trade practices and its notification untimely under Georgia law;

g. Whether Equifax's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Personal Information of Plaintiffs and Class members;

h. Whether Plaintiffs and Class members were injured and suffered damages or other acceptable losses because of Equifax's failure to reasonably protect its systems and data network; and

i. Whether Plaintiffs and Class members are entitled to relief.

55. **Typicality. Fed. R. Civ. P. 23(a)(3)**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of those of other Class members. Plaintiffs had their Personal Information compromised in the Data Breach. Plaintiffs' damages and injuries are akin to other Class members and Plaintiffs seeks relief consistent with the relief of the Class.

56. **Adequacy. Fed. R. Civ. P. 23(a)(4)**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Equifax to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

57. **Superiority. Fed. R. Civ. P. 23(b)(3)**. Consistent with Fed. R. Civ. P 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual Plaintiffs may not be sufficient to justify individual

litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Equifax, and thus, individual litigation to redress Equifax's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

58. **Injunctive and Declaratory Relief**. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

59. Likewise, 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:

a. Whether Equifax failed to timely notify the public of the Data Breach;

b. Whether Equifax owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

c. Whether Equifax's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

d. Whether Equifax failed to adequately comply with industry standards amounting to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiffs and the Class members; and,

f. Whether adherence to data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

60. Finally, all members of the proposed Classes are readily ascertainable. Equifax has access to information regarding the Data Breach, the time period of the Data Breach, and which individuals were potentially affected. Using this

information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

CAUSES OF ACTION

COUNT I – VIOLATION OF THE FAIR CREDIT REPORTING ACT
(On Behalf of Plaintiffs and the Nationwide Class)

61. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

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

63. 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 . . . ." 15 U.S.C. § 1681a(f).

64. Equifax is a consumer 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.

65. As a consumer reporting agency, 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).

66. 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).

67. The compromised data was a consumer report under the FCRA because it was a communication of information bearing on 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 the Class members' eligibility for credit.

68. 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 the Nationwide Class members' Personal Information. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

69. Equifax furnished the Nationwide 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.

70. The Federal Trade Commission ("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.[26]

[26] Statement of Commissioner Brill (Federal Trade Commission 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonestatement.pdf (last visited September 8, 2017).

71. 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, 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, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

72. 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 Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised 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 consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other members of the classes of their rights under the FCRA.

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

74. Plaintiffs and the Nationwide Class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide 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).

75. Plaintiffs and the Nationwide 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 II - NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the Separate Statewide Classes)

76. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

77. Upon accepting and storing the Personal Information of Plaintiffs and Class members in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Equifax knew that the Personal Information was private and confidential and should be protected as private and confidential.

78. Equifax owed a duty of care not to subject Plaintiffs, along with their Personal Information, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

79. Equifax owed numerous duties to Plaintiffs and to members of the Nationwide Class, including the following:

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

b. to protect Personal Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

80. Equifax also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard Personal Information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Personal Information. Furthering their dilatory practices, Equifax failed to provide adequate supervision and oversight of the Personal Information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Personal Information of Plaintiffs and Class Members, misuse the Personal Information and intentionally disclose it to others without consent.

81. Equifax knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including multiple prior breaches affecting Equifax and a well-publicized breach affecting 15 million customers of competitor Experian.

82. Equifax knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class members' Personal Information.

83. Equifax breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Personal Information of Plaintiffs and Class members.

84. Because Equifax knew that a breach of its systems would damage millions of individuals, including Plaintiffs and Class members, Equifax had a duty to adequately protect their data systems and the Personal Information stored therein.

85. Equifax had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' willingness to entrust Equifax with their Personal Information was predicated on the understanding that Equifax would take adequate security precautions. Many Class members had no say in whether Equifax used their Personal Information. Moreover, only Equifax had the ability to protect its systems and the Personal Information it stored on its systems from attack.

86. Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Personal Information. Equifax's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

87. Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard Plaintiff's and Class members' Personal Information and promptly notify them about the data breach.

88. Equifax breached its duties to Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Personal Information of Plaintiffs and Class members;

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

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class members' Personal Information both before and after learning of the Data Breach;

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

e. by failing to timely and accurately disclose that Plaintiffs' and Class members' Personal Information had been improperly acquired or accessed.

89. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect Personal Information of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure Personal Information of Plaintiffs and Class members during the time it was within Equifax possession or control.

90. The law further imposes an affirmative duty on Equifax to timely disclose the unauthorized access and theft of the Personal Information to Plaintiffs and the Class so that Plaintiffs and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information.

91. Equifax breached its duty to notify Plaintiffs and Class Members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiffs and Class Members and then by failing to provide Plaintiffs and Class Members information regarding the breach until September 2017. Instead, its executives disposed of at least $1.8 million worth of shares in the company after Equifax learned of the data breach but before it was publicly announced. To date, Equifax has not provided sufficient information to Plaintiffs and Class Members

regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

92. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect Personal Information of Plaintiffs and Class Members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure Personal Information of Plaintiffs and Class members during the time it was within Equifax's possession or control.

93. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Equifax prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their financial data and accounts.

94. Upon information and belief, Equifax improperly and inadequately safeguarded Personal Information of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Equifax's failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act,

namely the unauthorized access of Personal Information of Plaintiffs and Class members.

95. Equifax's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Personal Information; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Personal Information of Plaintiffs and Class members; and failing to provide Plaintiffs and Class members with timely and sufficient notice that their sensitive Personal Information had been compromised.

96. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their Personal Information as described in this Complaint.

97. As a direct and proximate cause of Equifax's conduct, Plaintiffs and the Class suffered damages including, but not limited to: damages arising from identity theft, tax fraud, and/or false or fraudulent charges stemming from the Data Breach, including late fees charges and unauthorized charges; 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.

COUNT III – NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the Separate Statewide Classes)

98. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

99. As set forth above, Equifax is required under the Fair Credit Reporting Act, 15 U.S.C. §§ 1681e, 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).

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

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

102. Equifax was also required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards: "(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." 15 U.S.C. § 6801(b).

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

104. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to

address incidents of unauthorized access to customer information in customer information systems." *See id*.

105. Further, when Equifax became aware of "unauthorized access to sensitive customer information," it should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible." *Id*.

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

107. Equifax also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law

enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

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

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

110. Likewise, 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 Personal Information. The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

111. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored, and the foreseeable consequences of a data breach at a

corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiffs and Class members.

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

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

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

115. As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiffs and Class members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs and Class members' Personal Information has also diminished the value of the Personal Information.

116. The damages to Plaintiffs and the Class members were a proximate, reasonably foreseeable result of Equifax's breaches of it's the applicable laws and regulations.

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

COUNT IV – BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the Separate Statewide Classes)

118. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

119. Equifax's privacy policies constitute an agreement between Equifax and individuals who provided their Personal Information to Equifax.

120. Equifax's privacy policy states, among other things, "We will not disclose your personal information to third parties except to provide you with the disclosure or service you request, or under certain circumstances as described in this policy."

121. Equifax breached its agreement with Plaintiffs and Class members to protect their Personal Information by (1) failing to implement security measures designed to prevent this attack, (2) failing to employ security protocols to detect the unauthorized network activity, and (3) failing to maintain basic security

measures such as complex data encryption so that if data were accessed or stolen it would be unreadable.

122. Plaintiffs and Class members have been damaged by Equifax's breach of its contractual obligations because their Personal Information has been compromised and they have suffered identity theft and fraud, and/or are at an increased risk for identity theft and fraud. Plaintiffs and the Class have been deprived of the value of their Personal Information and have lost money and property as a result of Equifax's unlawful and unfair conduct.

123. Plaintiffs individually and on behalf of the Class seek recovery for damages suffered by members of the class, equitable relief, and injunctive relief requiring Equifax and its agents to implement safeguards consistent with its contractual promises.

COUNT V – BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the Separate Statewide Classes)

124. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

125. Plaintiffs and many Class members entered into an implied contract with Equifax whereby consumers paid money and provided their Personal Information to Equifax in exchange for credit reporting services.

126. As part of this transaction, Plaintiffs' and Class members entered into implied contracts with Equifax pursuant to which Equifax agreed to safeguard and protect such Personal Information and to timely and accurately notify consumers if their data had been breached and compromised.

127. In entering into such implied contracts, Plaintiffs and Class members assumed that Equifax's data security practices and policies were reasonable and consistent with industry standards, and that Equifax would use part of the funds received from Plaintiffs and the Class members to pay for adequate and reasonable data security practices.

128. Plaintiffs and Class members would not have provided and entrusted their Personal Information to Equifax in the absence of the implied contract between them and Equifax to keep the information secure.

129. Plaintiffs and Class members fully performed their obligations under the implied contracts with Equifax.

130. Equifax breached its implied contracts with Plaintiffs and Class members by failing to safeguard and protect their Personal Information and by failing to provide timely and accurate notice that their Personal Information was compromised as a result of the Data Breach.

131. As a direct and proximate result of Equifax's breaches of the implied contracts, Plaintiffs and Class members sustained actual losses and damages as described herein.

COUNT VI – UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the Separate Statewide Classes)

132. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

133. Plaintiffs and the Class conferred a monetary benefit on Equifax as Equifax traded on and sold consumers' Personal Information in the form of credit reports and by other means in order to generate significant revenue for Equifax.

134. Equifax appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and the Class.

135. The revenue generated by Equifax should have been used by Equifax, in part, to pay for the costs of reasonable data privacy and security practices and procedures.

136. Under principles of equity and good conscience, Equifax should not be permitted to retain the money belonging to Plaintiffs and Class members because Equifax failed to implement (or adequately implement) the data privacy

and security practices and procedures that Plaintiffs and class members paid for wither knowingly or unknowingly.

137. Equifax should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds received by it. A constructive trust should be imposed upon all unlawful or inequitable sums received by Equifax traceable to Plaintiffs and Class members.

COUNT VII – VIOLATION OF THE GEORGIA FAIR BUSINESS PRACTICES ACT (Ga. Code Ann. § 10-1-390, *et seq.*)
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the Georgia Statewide Class)

138. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

139. Equifax, while operating in Georgia, engaged in unfair and deceptive consumer acts in the conduct of trade and commerce, in violation of Ga. Code Ann. § 10-1-390(a), and (b). This includes but is not limited the following:

a. Equifax failed to enact adequate privacy and security measures to protect the Class members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Equifax knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard the Class members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

d. Equifax knowingly omitted, suppressed, and concealed the inadequacy of its privacy and security protections for the Class members' Personal Information;

e. Equifax knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Class members' Personal Information, including but not limited to duties imposed by the FCRA, 15. U.S.C.§ 1681e, the GLBA, 15 U.S.C. § 6801 *et seq*., and the FTC Act;

f. Equifax failed to maintain the privacy and security of the Class members' Personal Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those

mentioned in the aforementioned paragraph, which was a direct and proximate cause of the Data Breach; and

g. Equifax failed to disclose the Data Breach to the Class members in a timely and accurate manner, in violation of § Ga. Code Ann 10-1-912.

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

COUNT VIII – VIOLATION OF THE GEORGIA SECURITY BREACH NOTIFICATION ACT (Ga. Code Ann. § 10-1-912, *et seq*).
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and the Georgia Statewide Class)

141. Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

142. Under Ga. Code Ann. § 10-1-912(a), "[a]ny information broker … that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have

been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay … .”

143. Under Ga. Code Ann. § 10-1-912(b), “[a]ny person or business that maintains computerized data on behalf of an information broker … that includes personal information of individuals that the person or business does not own shall notify the information broker … of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

144. Equifax is an information broker that owns or licenses computerized data that includes personal information, as defined by Ga. Code Ann. § 10-1-911.

145. In the alternative, Equifax maintains computerized data on behalf of an information broker that includes personal information that Equifax does not own, as defined by Ga. Code Ann. § 10-1-911.

146. Plaintiffs and the Class members’ Personal Information (including but not limited to names, addresses, and Social Security numbers) includes personal information covered under Ga. Code Ann. § 10-1-911(6).

147. Because Equifax was aware of a breach of its security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs and Class members’ Personal Information), Equifax had an obligation to disclose the

Data Breach in a timely and accurate fashion as mandated by Ga. Code Ann. § 10-1-912(a).

148. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated Ga. Code Ann. § 10-1-912(a).

149. As a direct and proximate result of Equifax's violations of Ga. Code Ann. § 10-1-912(a), Plaintiffs and Class members suffered the damages alleged herein.

150. Plaintiffs and Class members seek relief under Ga. Code Ann. § 10-1-912 including, but not limited to, actual damages and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes set forth herein, respectfully request the following relief:

a. That the Court certify this case as a class action pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and/or (c)(4) and, pursuant to Fed. R. Civ. P. 23(g), appoint the named Plaintiffs to be the Class representative and the undersigned counsel to be Class counsel;

b. That the Court award Plaintiffs and the Classes appropriate relief, including actual damages and restitution;

c. That the Court award Plaintiffs and the Classes pre-judgment and post-judgment interest; and

d. That the Court award Plaintiffs and the Classes such other favorable relief as allowable under law or at equity.

JURY DEMAND

Plaintiffs, on behalf of themselves and the Classes of all others similarly situated, hereby demand a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: September 8, 2017

Respectfully submitted,

THE BARNES LAW GROUP, LLC

/s/ Roy E. Barnes
Roy E. Barnes (No. 039000)
John R. Bevis (No. 056110)
J. Cameron Tribble (No. 754759)
31 Atlanta Street
Marietta, Georgia 30060
Tel.: 770-419-8505
Fax: 770-590-8958
roy@barneslawgroup.com
bevis@barneslawgroup.com
ctribble@barneslawgroup.com

Attorneys for Plaintiffs and the Class

STUEVE SIEGEL HANSON LLP

Norman E. Siegel*
Barrett J. Vahle*
J. Austin Moore*
460 Nichols Road, Suite 200
Kansas City, MO 64112
Tel: (816) 714-7100
Fax: (816) 714-7101
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com
**pro hac vice forthcoming*