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

APRIL MARDOCK, individually and on behalf of all others similarly situated, Plaintiff v. EQUIFAX, INC. Defendant.	Civil Action No. _____ Jury Trial Demanded

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff April Mardock individually and on behalf of the Classes defined below, alleges the following against Equifax, Inc. ("Equifax") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE CASE

1. Plaintiff bring this class action case against Defendant Equifax for its massive failure to secure and safeguard consumers' personally identifiable information ("PII") which Equifax collected from various sources in connection with the operation of its business as a consumer credit reporting agency, and for failing to

provide timely, accurate and adequate notice to Plaintiff and other consumers that their PII had been stolen and precisely what types of information were stolen.

2. On September 7, 2017, Equifax disclosed the occurrence of a cybersecurity incident ("Data Breach") in which unauthorized persons gained access to the PII of approximately 143 million U.S. consumers held by Equifax. Based on its investigation, Equifax stated that the period of unauthorized access lasted approximately ten (10) weeks, from mid-May through July 2017.

3. According to Equifax, the information accessed includes names, Social Security numbers, birth dates, addresses, and, in some instances, driver's license numbers. In addition, Equifax has admitted that credit card numbers for approximately 209,000 U.S. consumers, and certain other documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed.

4. Equifax has admitted that it discovered the Data Breach on July 29, 2017, but delayed informing the public until September 7, 2017. Equifax has not stated why it failed to disclose the Data Breach to consumers for nearly six weeks.

5. However, after Equifax learned of the Data Breach but before it was disclosed to the public, Equifax executives sold at least $1.8 million worth of shares of Equifax stock. It has been reported that its Chief Financial Officer John Gamble sold shares worth $946,374, its president of U.S. information solutions, Joseph

Loughran, exercised options to dispose of stock worth $584,099, and its president of workforce solutions, Rodolfo Ploder, sold $250,458 of stock on August 2, 2017.

6. Plaintiff brings this action on behalf of herself and of the class consisting of all consumers whose PII was accessed during the Data Breach (the "Class").

7. Equifax could and should have prevented this Data Breach. Data breaches at other companies, including one of its major competitors, Experian, have occurred, and Equifax is keenly aware of the need for data security and the devastating consequences of identity theft: indeed, Equifax offers, for a monthly fee, various plans supposedly designed to protect consumers from the consequences of identity theft and credit fraud.

8. Equifax has stated that criminals exploited a U.S. website application vulnerability in order to perpetrate the Data Breach. It has been reported that the specific vulnerability exploited in the Data Breach was one that was widely known among data security professionals for at least several months prior to the Data Breach. Moreover, patches and other solutions to prevent or mitigate the exploitation of the identified vulnerability were widely available prior to the Data Breach.

9. The Data Breach was the foreseeable result of Equifax's inadequate approach to data security and protection of the PII that it collected during the course of its business.

10. Equifax violated the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard PII, failing to take reasonable steps to prevent the Data Breach from occurring, failing to monitor and detect the Data Breach on a timely basis, and failing to provide timely notice after learning of the Data Breach. As a result of the Data Breach, the PII of the Plaintiff and Class members has been exposed to criminals for misuse. As a direct result of the Data Breach, Plaintiff and Class members suffered, or are likely to suffer, injuries including the unauthorized use of their PII; costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; loss of use of and access to account funds and costs associated with inability to obtain money from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations; costs associated with time spent and the loss of productivity or the enjoyment

of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach; and other injuries as more fully set forth below.

11. The injuries to the Plaintiff and Class members were directly and proximately caused by Equifax's failure to implement or maintain adequate data security measures for PII, failure to timely detect the Data Breach, and failure to timely notify Plaintiff and the Class members after learning of the Data Breach.

12. Further, Plaintiff retains a significant interest in ensuring that her PII, which, while stolen, also remains in the possession of Equifax, is protected from further breaches, and seeks to remedy the harms she has suffered on behalf of herself and other Class members.

13. Plaintiff brings this action to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff seeks the following remedies, among others: reimbursement of out-of-pocket losses, other compensatory damages, any available statutory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

JURISDICTION AND VENUE

14. 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. There are more than 100 putative class members. And, at least some members of the proposed Class have a different citizenship from Equifax.

15. This Court has personal jurisdiction over Equifax because Equifax is a citizen of Georgia, maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia and such contacts relate to this action. Equifax intentionally availed itself of this jurisdiction by marketing and selling products and services and by accepting and processing payments for those products and services within Georgia.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Equifax's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff' claims occurred in this District.

PARTIES

17. Plaintiff April Mardock is a citizen and resident of the state of Washington. Plaintiff is a victim of the Data Breach. Plaintiff has long been concerned about digitally available PII and knows the dangers of identity theft

in the digital age. Since February 2015, Plaintiff has been a subscriber to Equifax's Premier Family Plan, and has paid Equifax $30 per month for this service. This service was touted as a credit monitoring and identity theft protection plan. In connection with this plan, Plaintiff has provided Equifax with a copy of her driver's license, which contains PII including her name, address, height, weight, eye color, hair color and drivers' license number. After the Data Breach was announced, Equifax encouraged concerned consumers to check if their PII was stolen by entering information on an Equifax website. Plaintiff utilized the website and received the message from Equifax that "Based on the information provided, we believe that your personal information may have been impacted by this incident." Upon information and belief, those whose information was not taken were expressly told by Equifax that the information was not taken. Accordingly, Equifax's "may" in fact indicates that information was taken, or that Equifax cannot confirm, as it claims for some, that the information was not taken. Since the Data Breach, Plaintiff Mardock has spent time and effort monitoring her financial accounts.

18. Defendant Equifax, Inc. is a Delaware corporation with its principal place of business located at 1550 Peachtree Street NE, Atlanta, Georgia 30309.

Equifax, Inc. may be served through its registered agent, Shawn Baldwin, at its principal office address identified above.

STATEMENT OF FACTS

A. The Data Breach May Be The Most Severe in History In Terms of Impact on Consumers.

19. Equifax is one of three nationwide credit-reporting companies that track and rate the financial history of U.S. consumers. The companies are supplied with data about loans, loan payments and credit cards, as well as information on everything from child support payments, credit limits, missed rent and utilities payments, addresses and employer history. All this information, and more, factors into credit scores, which are provided by Equifax as well as other companies based on information from Equifax.

20. Credit scores are critically important to consumers because a credit score effects their access to credit and determines how much they pay for credit, including mortgages and credit cards.

21. Equifax states that the Data Breach affected the PII of over 143 million U.S. consumers. The estimated U.S. adult population is 249 million.

22. According to Fox News, "[t]his data breach almost certainly will rank among the largest in U.S. history, leaving millions of Americans at risk for identity theft."[1]

23. Unlike other data breaches, many people affected by the Equifax breach are not customers of Equifax and may not be aware that Equifax has their PII. Equifax gets its data from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies, as well as by purchasing public records. In addition, as noted above, Equifax sells various credit-protection services.

24. Included among the stolen files was a treasure trove of personal data: names, dates of birth, Social Security numbers, and addresses. In some cases -- Equifax states around 209,000 -- the records also included actual credit card numbers. Documentation about disputed charges was also leaked. Those documents contained additional personal information on around 182,000 Americans.

25. PII is valuable. A "cyber black market" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. PII is valuable to identity thieves because they can use victims' personal data for nefarious

[1] http://www.foxbusiness.com/features/2017/09/08/equifax-breach-how-to-protect-yourself.html (last visited Sept. 12, 2017).

purposes such as opening new financial accounts and taking out loans in another person's name, incurring charges on existing accounts, or cloning ATM, debit, or credit cards.

26. The Equifax Data Breach is uniquely damaging due to the combination of the number of consumers affected and the type of information involved. The Los Angeles times reported, for example: "The data now at large includes names, Social Security numbers, birthdates, addresses and driver's license numbers, all of which can be used fraudulently to validate the identity of someone trying to open a bank or credit account in another person's name. In some cases, Equifax says, the security questions and answers used on some websites to verify users' identity may also have been exposed. Having that information in hand would allow hackers to change their targets' passwords and other account settings."[2]

27. According to respected technology website Ars Technica:

> The breach Equifax reported Thursday, however, very possibly is the most severe of all for a simple reason: the breath-taking amount of highly sensitive data it handed over to criminals. By providing full names, Social Security numbers, birth dates, addresses, and, in some cases, driver license numbers, it provided most of the information banks, insurance companies, and other businesses use to confirm consumers are who they claim to be. The theft, by criminals who exploited a security

[2] http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html (last visited Sept. 12, 2017).

> flaw on the Equifax website, opens the troubling prospect the data is now in the hands of hostile governments, criminal gangs, or both and will remain so indefinitely.[3]

B. Equifax Could And Should Have Prevented The Data Breach.

28. Equifax had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

29. Had Equifax remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Equifax would have prevented the Data Breach and, ultimately, the theft of its customers' PII.

30. At all relevant times, Equifax was well-aware that the PII it collected, maintained and stored is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud. In fact, Equifax states on its website:

> As a trusted steward of consumer and business information, Equifax employs strong data security and confidentiality standards on the data we provide and on the access to that data. We maintain a highly sophisticated data information network that includes advanced security, protections and redundancies.

[3] https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/ (last visited Sept. 12, 2017).

> The Equifax network is reviewed on a continual basis by external security experts who conduct intrusion testing, vulnerability assessments, on-site inspections, and policy/incident management reviews. Equifax annually completes a SAS 70 Type II audit and receives TruSecure's accredited security certification. Additionally, Equifax conducts internal security reviews on a weekly basis.

31. Notwithstanding these representations, Forbes reports[4] that Equifax itself has a history of "security fails," including:

a. Equifax was previously sued over "a May 2016 incident in which Equifax's W-2 Express website had suffered an attack that resulted in the leak of 430,000 names, addresses, social security numbers and other personal information of retail firm Kroger."

b. In May 2017, an Equifax informed its customers that "hackers had used personal information to guess personal questions of employees in order to reset the 4-digit PIN given and stolen tax data. In its disclosure, Equifax said the unauthorized access to the information occurred between April 17, 2016 and March 29 the following year."

c. "In January 2017, Equifax was forced to confess to a data leak in which credit information of a 'small number' of customers at partner

[4] https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#1e547549677c (last visited Sept. 12, 2017).

LifeLock had been exposed to another user of the latter's online portal."

d. In 2014, Equifax reported to the New Hampshire attorney general that between April 2013 and January 2014, an "IP address operator was able to obtain the credit reports using sufficient personal information to meet Equifax's identity verification process."

32. Moreover, Equifax was aware of a series of highly publicized major data breaches at other companies, including Equifax's competitor, Experian.[5]

33. Despite Equifax's knowledge of major data breaches, including its own, and the value of PII on the black market, Equifax's approach to maintaining the privacy and security of the PII of Plaintiff and Class members was lackadaisical, cavalier, reckless, or at the very least, negligent.

34. According to Equifax's report on September 7, 2017, the Data Breach was discovered on July 29th. The perpetrators gained access by "[exploiting] a [...] website application vulnerability" on one of the company's U.S.-based servers. The hackers were then able to access the PII of Plaintiff and the Class.

[5] See, e.g., https://www.usatoday.com/story/tech/2017/09/07/nations-biggest-hacks-and-data-breaches-millions/644311001/ (last visited Sept. 12, 2017).

35. According to a September 8, 2017, article by the New York Post, the breach was perpetuated by exploitation of a software flaw within a third-party programming framework utilized by many large companies to build web applications. The software system, called "Apache Struts," was compromised in March 2017. By May 2017, when the Data Breach began, software patches to neutralize the March 2017 Struts vulnerability had existed for months. In addition to the software patch, additional tools provided by software companies existed that would have mooted any Struts vulnerability by providing filtering of attack traffic prior to exposure to the Struts-enabled server. In short, the Data Breach could have been prevented had Equifax utilized reasonable care.

C. Plaintiff Has Been Damaged By the Data Breach.

36. The ramifications of Equifax's failure to keep Plaintiff's and Class members' PII secure are severe.

37. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by her PII being placed in the hands of criminals who have already, or will imminently, misuse such information

38. Additionally, Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII – a form of intangible property that was compromised in and as a result of the Data Breach.

39. Moreover, Plaintiff has a continuing interest in ensuring that her private information, which remains in the possession of Equifax, is protected and safeguarded from future breaches.

40. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[6] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[7] As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[8]

[6] 17 C.F.R § 248.201 (2013).
[7] *Id.*
[8] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Sept. 12, 2017).

As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[9]

41. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[10]

42. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend time and money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[11]

43. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

---

[9] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Sept. 12, 2017).

[10] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited Sept. 12, 2017).

[11] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Sept. 12, 2017).

> [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. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[12]

44. Plaintiff and members of the Class 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 PII.

45. The Equifax Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiff' and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

46. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been

[12] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited Sept. 12, 2017).

placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time, which they otherwise would have dedicated to other life demands, such as work, 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. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable. For many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency's slippage, as is the case here.

47. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff' and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiff' and Class members' information on the black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their PII;

f. loss of privacy;

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

h. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

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

obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. the loss of productivity and value of their time spent to attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

48. Equifax has not offered customers appropriate credit monitoring or identity theft protection services, despite the fact that it is well known and acknowledged by the government that damage and fraud from a data breach can take many years to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Equifax's actions have created for Plaintiff and Class members, is ascertainable and is a determination appropriate for the trier of fact. Equifax has also not offered to cover any of the damages sustained by Plaintiff or Class members.

49. While the PII of Plaintiff and members of the Class has been stolen, Equifax continues to hold PII of consumers, including Plaintiff and Class members. Particularly because Equifax has demonstrated an inability to prevent a breach, Plaintiff and members of the Class have an undeniable interest in insuring that their PII is secure, remains secure, and is not subject to further theft.

D. Equifax's Inadequate Response and Notification of the Breach.

50. In addition to waiting approximately six weeks to disclose the breach publicly, Equifax's attempts at notifying consumers of the breach has been confusing and contradictory, providing unreliable and inconsistent information. As reported on respected cybersecurity site Krebsonsecurity.com on September 8, 2017:

> As noted in yesterday's breaking story on this breach, the Web site that Equifax advertised as the place where concerned Americans could go to find out whether they were impacted by this breach — equifaxsecurity2017.com —is completely broken at best, and little more than a stalling tactic or sham at worst.
>
> In the early hours after the breach announcement, the site was being flagged by various browsers as a phishing threat. In some cases, people visiting the site were told they were not affected, only to find they received a different answer when they checked the site with the same information on their mobile phones.
>
> Others (myself included) received not a yes or no answer to the question of whether we were impacted, but instead a message that credit monitoring services we were eligible for were not available and

> to check back later in the month. The site asked users to enter their last name and last six digits of their SSN, but at the prompting of a reader's comment I confirmed that just entering gibberish names and numbers produced the same result as the one I saw when I entered my real information: Come back on Sept. 13.[13]

51. In addition, Equifax initially attempted to strong-arm consumers into agreeing to waive their legal rights by including an arbitration clause and class action waiver in a "terms of service" link on the webpage where it offered consumers (inadequately short) one free year of credit monitoring and identity protection services.

52. The effort was widely condemned by the media and public, forcing Equifax to retract it. In the Frequently Asked Questions section of the Equifax website, Equifax now states:

> To confirm, enrolling in the free credit file monitoring and identity theft protection products that we are offering as part of this cybersecurity incident does not prohibit consumers from taking legal action. We have already removed that language from the Terms of Use on the site www.equifaxsecurity2017.com. The Terms of Use on www.equifax.com do not apply to the TrustedID Premier product being offered to consumers as a result of the cybersecurity incident. Again, to be as clear as possible, we will not apply any arbitration clause or class action waiver against

[13] *Equifax Breach Response Turns Dumpster Fire*, https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/ (last visited Sept. 11, 2017).

> consumers for claims related to the free products offered in response to the cybersecurity incident or for claims related to the cybersecurity incident itself.

https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last visited Sept. 11, 2017)

CLASS ALLEGATIONS

53. Plaintiff seeks relief on behalf of herself and as representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons residing in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017 (the "Nationwide Class").

54. Plaintiff also brings this action pursuant to Washington law on behalf of herself and a class of all other persons similarly situated pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), defined as follows:

> All persons residing in Washington whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017 (the "Washington Class" which, together with the Nationwide Class will be referred to as the "Classes" or the "Class").

55. Excluded from each of the above Classes are Equifax and any of 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.

56. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

57. Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

58. **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 Plaintiff at this time, the proposed Class includes approximately 143 million individuals whose PII was compromised in the 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.

59. **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 PII;

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 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 PII of Plaintiff and Class members;

h. Whether Plaintiff and Class members were injured and suffered losses because of Equifax's failure to reasonably protect PII; and,

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

60. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff's PII was compromised in the Data Breach. Plaintiff's damages and injuries are akin to other Class members and Plaintiff seeks relief consistent with the relief of the Class.

61. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Equifax to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

62. **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 Plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff 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.

63. **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.

64. 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 Breach;

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

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 PII of Plaintiff and the Class members; and,

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

65. 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 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.

COUNT I
NEGLIGENCE

(On Behalf Of Plaintiff And The Nationwide Class, Or, Alternatively, Plaintiff And The Washington Class)

66. Plaintiff restates and realleges Paragraphs 1 through 65 as if fully set forth herein.

67. Upon accepting and storing the PII of Plaintiff and Class Members in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiff 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 PII was private and confidential and should be protected as private and confidential.

68. Equifax owed a duty of care not to subject Plaintiff and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

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

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

b. to protect PII 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.

70. Equifax had a special relationship with Plaintiff and Class members by virtue of its obtaining and storing their PII. Moreover, only Equifax had the ability to protect its systems and the PII it stored on them from attack.

71. Equifax's conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PII. 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.

72. Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard Plaintiff's and Class members' PII and promptly notify them about the Data Breach.

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

74. Equifax knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including the breach at Experian.

75. Equifax knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' PII.

76. Equifax breached its duties to Plaintiff and Class members in numerous ways, including:

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

b. by failing to use reasonable care to adequately protect and secure PII of Plaintiff and Class members during the time it was within Equifax's possession or control;

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

d. by failing to provide adequate supervision and oversight of the PII 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 PII of Plaintiff and Class members, misuse the PII and intentionally disclose it to others without consent;.

e. by knowingly disregarding standard information security principles, despite obvious risks, both before and during the period of the Data Breach; and

f. by failing to timely and accurately disclose that Plaintiff's and Class members' PII had been improperly acquired or accessed.

77. Equifax breached its duty to notify Plaintiff and Class members of the unauthorized access by waiting six weeks after learning of the Data Breach to notify Plaintiff and Class members of the Data Breach. To date, Equifax has not provided sufficient information to Plaintiff and Class members regarding the

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

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

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

80. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

81. As a direct and proximate cause of Equifax's conduct, Plaintiff and the Class 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 and Class members; damages arising from Plaintiff's and Class members' 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 charges and foregone cash back rewards; 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 II
NEGLIGENCE PER SE

(On Behalf Of Plaintiff And The Nationwide Class, Or, Alternatively, Plaintiff And The Washington Class)

82. Plaintiff restates and realleges Paragraphs 1 through 81 as if fully set forth herein.

83. 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.

84. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of PII 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 Plaintiff and Class members.

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

86. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

87. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ

reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

88. As a direct and proximate result of Equifax's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries arising from Plaintiff's and Class members' 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 charges and foregone cash back rewards; 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
VIOLATION OF GEORGIA FAIR BUSINESS PRACTICES ACT O.C.G.A. § 10-1-390, *ET SEQ*.

(On Behalf Of Plaintiff And The Nationwide Class)

89. Plaintiff restates and realleges Paragraphs 1 through 88 as if fully set forth herein.

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

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

92. Plaintiff and Class members entrusted Equifax with their PII.

93. 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 Plaintiff and 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.

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

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

96. As a direct and proximate result of Equifax's violation of the GFBPA, Plaintiff and 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 and Class members; damages arising from Plaintiff's and 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; 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.

97. Also as a direct result of Equifax's knowing violation of the GFBPA, Plaintiff and 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 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.

98. Plaintiff brings this action on behalf of herself 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 and 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.

99. Plaintiff and 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 IV
VIOLATIONS OF GEORGIA DATA BREACH STATUTE O.C.G.A. § 10-1-912, *ET SEQ*.

(On Behalf Of Plaintiff And The Nationwide Class)

100. Plaintiff restates and realleges Paragraphs 1 through 99 as if fully set forth herein.

101. Georgia has enacted a data breach statute, which generally applies to any person or business conducting business within the state that owns or licenses computerized data containing PII. If the PII is acquired or accessed in a way that compromises its security or confidentiality, the covered entity must notify the affected individuals in the most expedient time and manner possible and without unreasonable delay.

102. The Equifax Data Breach constituted a security breach that triggered the notice provisions of the Georgia data breach statute and the PII taken includes categories of personal information protected by the data breach statutes.

103. Equifax unreasonably delayed informing Plaintiff and members of the Class about the Data Breach after Equifax knew or should have known that the Data Breach had occurred.

104. Plaintiff and Class members were damaged by Equifax's failure to comply with the data breach statute.

105. Had Equifax provided timely and accurate notice, Plaintiff and 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, taken security precautions in time to prevent or minimize identify theft, or could have avoided using uncompromised payment cards during subsequent purchases.

106. Equifax's failure to provide timely and accurate notice of the Data Breach violated O.C.G.A. § 10-1-912(a), *et seq*.

107. Plaintiff and members of Class seek all remedies available under the data breach statute, including but not limited to damages, equitable relief, including injunctive relief, treble damages, reasonable attorney fees and costs, as provided by the applicable laws.

COUNT V
FAILURE TO TIMELY DISCLOSE BREACH UNDER RCW 19.255.010

(On Behalf Of The Washington Class)

108. Plaintiff restates and realleges Paragraphs 1 through 107 as if fully set forth herein.

109. Equifax is a business conducting business in Washington and owns or licenses computerized data that includes personal information, as defined under RCW 19.255.010.

110. In mid-May 2017, Equifax's computer system storing personal and financial information was breached, and unauthorized individuals gained access to the information.

111. Equifax knew or should have known that the breach occurred, but due to its own negligent monitoring of its information systems, it did not discover the breach until July 29, 2017.

112. Equifax has yet to adequately notify persons whose data was breached.

113. Equifax's failure to detect and disclose the breach constituted an unreasonable delay.

114. As a direct and proximate result of Equifax's failure to provide reasonably prompt disclosure, Plaintiff and the Class have suffered damages.

COUNT VI
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT RCW 19.86.010 *ET SEQ.*

(On Behalf Of The Washington Class)

115. Plaintiff restates and realleges Paragraphs 1 through 114 as if fully set forth herein.

116. The conduct of Defendant as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to accepting and storing Plaintiff's and the Class members' personal and financial information but failing to

take reasonable steps to protect it in violation of industry standards and best practices. Equifax also violated consumer expectations to safeguard personal and financial information and failed to tell consumers that it did not have reasonable and best practices, safeguards, and data security in place.

117. Equifax also violated the Washington Consumer Protection Act by failing to immediately notify Plaintiff and the Class of the Data Breach. If Plaintiff and the Class had been notified in a timely and appropriate manner, they could have taken precautions to better safeguard their personal and financial information and mitigate damages flowing from the Data Breach.

118. Defendant's actions as set forth above occurred in the conduct of trade or commerce.

119. To establish that an act is a "consumer" transaction, it must be likely that "additional Plaintiffs have been or will be injured in exactly the same fashion." *Hangman Ridge Training Stables, Inc. v. Safeco Title Ins. Co.*, 105 Wn.2d 778, 790 (1986).

120. Plaintiff was injured exactly the same way as millions of other Equifax customers.

121. In a consumer transaction, the following factors determine whether the transaction "impacts the public interest":

> Were the alleged acts committed in the course of defendant's business? (2) Are the acts part of a pattern or generalized course of conduct? (3) Were repeated acts committed prior to the act involving plaintiff? (4) Is there a real and substantial potential for repetition of defendant's conduct after the act involving plaintiff? (5) If the act complained of involved a single transaction, were many consumers affected or likely to be affected by it? *Id*.

122. Defendant conducted the practices alleged herein in the course of its business pursuant to standardized practices that it engaged in both before and after the Plaintiff in this case were harmed, and many consumers were affected.

123. As a direct and proximate result of Equifax's negligence and misconduct described in this complaint, Plaintiff and the Class were or are likely to be injured in fact by: (a) fraudulent charges; (b) theft of their personal and financial information; (c) costs associated with the detection and prevention of identity theft; (d) costs associated with the detection and prevention of unauthorized use of their financial accounts; (e) costs associated with being unable to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts; and (f) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach, all of which have an ascertainable monetary value to be proven at trial.

124. Defendant's conduct proximately caused Plaintiff's and the Class members' injuries.

125. Defendant is liable to Plaintiff and the Class for damages in amounts to be proven at trial, including attorneys' fees, costs, and treble damages.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all members of the Classes 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 Plaintiff and her Counsel to represent the Nationwide Class, or in the alternative the separate Washington Class;

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

Plaintiff demands a jury trial on all issues so triable.

This 12th day of September 2017.

/s/ James M. Evangelista
James M. Evangelista
Georgia Bar No. 707807
David J. Worley
Georgia Bar No. 776665
Kristi Stahnke McGregor
Georgia Bar No. 674012
EVANGELISTA WORLEY, LLC
8100 A. Roswell Road
Suite 100
Atlanta, GA 30350
Tel: (404) 205-8400
Facsimile: (404) 205-8395
david@ewlawllc.com
jim@ewlawllc.com
kristi@ewlawllc.com

MILBERG LLP

Ariana J. Tadler
Pro Hac Vice Application Forthcoming
Andrei V. Rado
Pro Hac Vice Application Forthcoming
Henry Kelston
Pro Hac Vice Application Forthcoming
One Pennsylvania Plaza
50th Floor
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (312) 346-0022
atadler@milberg.com
arado@milberg.com
hkelston@milberg.com

Counsel for Plaintiff 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)

APRIL MARDOCK, Individually and on behalf of all Others Similarly Situated,

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF King County, WA
(EXCEPT IN U.S. PLAINTIFF CASES)

DEFENDANT(S)

EQUIFAX, INC.

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT _____
(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)

James M. Evangelista, David J. Worley and Kristi Stahnke McGregor
EVANGELISTA WORLEY LLC
8100A Roswell Rd., Suite 100, Atlanta, GA 30350
Ph: (404)205-8400; jim@ewlawllc.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 pursuant to 28 U.S.C. § 1332(d)(2) whereby defendant, among other things, failed to adequately protect Plaintiffs' personal and credit data in violation of statutory and common law.

(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 _____ (Referral) NATURE OF SUIT _____ CAUSE OF ACTION _____

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK
- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK
- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☐ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 210 LAND CONDEMNATION
- ☐ 220 FORECLOSURE
- ☐ 230 RENT LEASE & EJECTMENT
- ☐ 240 TORTS TO LAND
- ☐ 245 TORT PRODUCT LIABILITY
- ☐ 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK
- ☐ 310 AIRPLANE
- ☐ 315 AIRPLANE PRODUCT LIABILITY
- ☐ 320 ASSAULT, LIBEL & SLANDER
- ☐ 330 FEDERAL EMPLOYERS' LIABILITY
- ☐ 340 MARINE
- ☐ 345 MARINE PRODUCT LIABILITY
- ☐ 350 MOTOR VEHICLE
- ☐ 355 MOTOR VEHICLE PRODUCT LIABILITY
- ☑ 360 OTHER PERSONAL INJURY
- ☐ 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☐ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK
- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK
- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK
- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK
- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK
- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK
- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK
- ☐ 830 PATENT
- ☐ 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (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 $ TBD

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

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE _____ DOCKET NO. _____

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.

SIGNATURE OF ATTORNEY OF RECORD DATE 9/12/2017