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

KURTIS ST. CLAIR, KYLE MCCLURE, , JEREMIAH SMITH, COURTNEY D. SMITH, JOSH RUPNOW, individually and on behalf of all others similarly situated, Plaintiff v. EQUIFAX, INC. Defendant.	Case No.

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiffs Kurtis St. Clair, Kyle McClure, Jeremiah Smith, Courtney D. Smith and Josh Rupnow (the "Plaintiffs"), individually and on behalf of the Classes defined below, allege the following against Equifax, Inc. ("Equifax") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE CASE

1. Defendant Equifax is one of the largest consumer credit reporting agencies in the world. Its core business – the very reason for its existence – is the collection, aggregation, and sale of the personally identifiable information ("PII") of hundreds of millions of U.S. consumers, usually without their knowledge or consent.

2. Plaintiffs bring this class action case against Equifax for its massive failure to secure and safeguard consumers' PII, which Equifax collected from various sources as part of its regular business operations, and for failing to provide timely, accurate and adequate notice to

Plaintiffs and other consumers that their PII had been stolen and precisely what types of information were stolen. Plaintiffs bring this action on behalf of themselves and of the class consisting of all consumers whose PII was accessed during the Data Breach (as defined below), (hereinafter the "Class").

3. 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. On October 2, 2017, Equifax disclosed that 2.5 million additional people were impacted by the breach.

4. 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.

5. 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.

6. 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. The Data Breach has severely impacted Equifax's stock price, which fell from approximately $143 per share in September 7, 2017, to $93 on September 15, a decline of 35% that wiped out $6 billion in market capitalization.

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 woefully inadequate data security, which resulted in its failure to adequately protect the PII of Plaintiffs and Class members.

10. Equifax violated the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard PII, to take reasonable steps to prevent the Data Breach from occurring, to monitor and detect the Data Breach on a timely basis, and to provide timely notice after learning of the Data Breach.

As a result of the Data Breach, the PII of the Plaintiffs and Class members have been exposed to criminals for misuse. As a direct result of the Data Breach, Plaintiffs 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 Plaintiffs 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 Plaintiffs and the Class members after learning of the Data Breach.

12. Further, Plaintiffs retain a significant interest in ensuring that their PII, which, while stolen, also remains in the possession of Equifax, is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and other Class members.

13. Plaintiffs bring this action to remedy these harms on behalf of themselves and all members of the Class. Plaintiffs seek 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 Plaintiffs' claims occurred in this District.

PARTIES

17. Plaintiff Kurtis St. Clair is a citizen and resident of the state of Michigan. Following Equifax's announcement of the Data Breach, Plaintiff checked on Equifax's website whether his PII was taken, and was informed that "your personal information may have been impacted by this incident. " In May 2017, Plaintiff's Chase Sapphire credit card was used in two transactions unauthorized by him. Chase cancelled the card once it had become aware that the transactions were not authorized, and issued him a new card. This caused Plaintiff to miss the payment of bills that Plaintiff had set-up to auto-charge. Plaintiffs' telephone carrier, Verizon, informed him that his scheduled payments could not be processed. In addition, Plaintiff's missed his home insurance and auto insurance payments because these were also linked to his cancelled

Chase card, and Plaintiff had to contact several other service providers to update them with his new card information (these included his propane and electricity suppliers, respectively). Plaintiff was greatly inconvenienced by spending significant time in resolving these issues.

18. Plaintiff Kyle McClure is a citizen and resident of the state of California. Following Equifax's announcement of the Data Breach, Plaintiff checked on Equifax's website whether his PII was taken, and was informed that "your personal information may have been impacted by this incident. " In the summer, Plaintiff began to explore the purchase of his first home. He shopped for loans with Quicken Loans, a popular online mortgage lender. He was told that he would need a credit score of 600 to qualify for a loan that would allow him to buy a home with the characteristics he wanted. In August 2017, Plaintiff learned through Credit Karma, an online provider of free credit reports, that his credit score was 602. However, within a month his credit report had dropped to 562 as result of unauthorized "hard inquiries" which are credit checks performed by institutions when the consumer applies for credit. Hard inquiries lower one's credit score. Plaintiff's credit report reflected hard inquiries that he never authorized, including from: Best Buy for an increase in Plaintiff's line of credit that he never requested and Citibank. These unauthorized inquiries occurred after the Data Breach.

19. Plaintiff Jeremiah Smith is a citizen and resident of the state of Texas. Following Equifax's announcement of the Data Breach, Plaintiff Smith checked on Equifax's website whether his PII was taken, and he was informed that "your personal information may have been impacted by this incident." To protect himself from the high risk of fraud and identity theft posed by the Data Breach, Plaintiff Smith froze his credit with all three major credit agencies at a total cost of $20.37. In addition, he obtained and reviewed a free annual credit report.

20. Plaintiff Courtney D. Smith is a citizen and resident of Missouri. Following Equifax's announcement of the Data Breach, Ms. Smith checked on Equifax's website whether her PII was taken, and was informed that "your personal information may have been impacted by this incident." In September 2017, a fraudulent charge for a purchase of $4000.39 at Costco appeared on Ms. Smith's Citibank credit statement. After confirming with Costco that the charge was not made under her Costco account, Ms. Smith made calls to Citibank to arrange for her credit card account to be closed and to have a new credit card issued. Ms. Smith froze her credit with Equifax on September 11, 2017. Ms. Smith was not the victim of identity theft or fraudulent credit charges prior to the Data Breach.

21. Plaintiff Josh Rupnow is a citizen and resident of the state of Washington. Since the Data Breach, two debit cards and one credit card have been fraudulently issued in his name, all tied to his Chase checking account. Charges for a social networking site called Badoo, which Mr. Rupnow has never used, have appeared multiple times on the debit cards. Mr. Rupnow has not been reimbursed for $29.95 of these charges. In addition, a Credit One credit card was fraudulently opened in Mr. Rupnow's name, showing a cash advance of $200 in Las Vegas. With time and effort, he was able to have this charge reversed. In May 2017, for the first time, Mr. Rupnow began receiving automated phone calls purported to be from the Internal Revenue Service. As a result of these events following the Data Breach, Mr. Rupnow signed up for credit monitoring with Experian.

22. 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.

23. Equifax is a nationwide credit-reporting company that tracks and rates the financial history of U.S. consumers. The companies are supplied with data about loans, loan payments and credit card accounts, and information on everything from child support payments, credit limits, missed rent and utilities payments, addresses to employment history. All of this information, and more, factors into credit scores, which are provided by Equifax and other companies using information from Equifax.

24. Financial histories and credit scores, which include and are based in part on consumers' PII, are critically important to consumers because they determine one's access to, and cost of, credit, including mortgage loans, credit cards, and car loans. In addition, such information is often considered in non-credit-related decisions, such as hiring decisions by prospective employers.As a result, the misappropriation and misuse of consumers' PII can have serious, longlasting and wide-ranging negative effects on consumers victimized by the Data Breach, often without the victims even being aware of those effects.

25. Equifax states that the Data Breach affected the PII of over 145 million U.S. consumers. The estimated U.S. adult population is 249 million.

26. 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]

27. 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

[1] http://www.foxbusiness.com/features/2017/09/08/equifax-breach-how-to-protect-yourself.html (last visited Nov. 16, 2017).

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.

28. 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.

29. 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 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.

30. 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]

31. According to respected technology website Ars Technica:

[2] http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html (last visited Nov. 16, 2017).

> The breach Equifax reported … 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 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.

32. The Data Breach could easily have been prevented. Equifax had the resources to prevent a breach, but neglected to adequately invest in data security, and to guard against a critical vulnerability warned about on March 10, 2017, more than two months before the devastating hack occurred.

33. 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 theft of the PII.

34. 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.
>
> 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

[3] https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/ (last visited Nov 16, 2017).

security certification. Additionally, Equifax conducts internal security reviews on a weekly basis.

35. 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, 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 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."

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

---

[4] https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#1e547549677c (last visited Nov. 17, 2017).

37. 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 Plaintiffs and Class members was lackadaisical, cavalier, reckless, or at the very least, negligent.

C. The Vulnerability That Allowed the Hack Was Well Publicized and Warned About Within The IT Security Community Months Before The Equifax Breach And Could Have Been Easily Remedied

38. According to Equifax's announcement 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 then accessed the PII of Plaintiffs and the Class.

39. On September 13, 2017, Equifax disclosed on its site the specifics about the security vulnerability that allowed the hack:

> Updated information on U.S. website application vulnerability.
>
> Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.[6]

40. The Apache Struts CVE-2017-5638 vulnerability was warned about by the National Institute of Standards and Technology ("NIST"), which is part of the U.S. Department of

---

[5] See, e.g., https://www.usatoday.com/story/tech/2017/09/07/nations-biggest-hacks-and-data-breaches-millions/644311001/ (last visited Nov. 16, 2017).

[6] https://www.equifaxsecurity2017.com/ (last visited Nov. 16, 2017).

Commerce, on March 10, 2017. Among other things, the NIST posts public warnings of cybersecurity threats, and ranks them in terms of seriousness on a scale of 1 to 10, with 10 being the highest risk level. Cybersecurity professionals regularly check the NIST warnings. The vulnerability identified by Equifax as responsible for the hack was classified by the NIST as a "10 critical, " on March 10. *See* Exhibit A.

41. The vulnerability warning was well publicized. For example, *PC World*, a publication available to the general public, reported on the Apache Struts in an article by Lucian Constantin on its website on March 9, 2017, noting that the vulnerability was easy to exploit, and must be addressed as a high priority:

> **Hackers exploit Apache Struts vulnerability to Compromise Corporate Web Servers**
>
> **The vulnerability allows attackers to execute malicious code on servers without authentication**
>
> Attackers are widely exploiting a recently patched vulnerability in Apache Struts that allows them to remotely execute malicious code on web servers.
>
> Apache Struts is an open-source web development framework for Java web applications. It's widely used to build corporate websites in sectors including education, government, financial services, retail and media.
>
> ***On Monday, the Apache Struts developers fixed a high-impact vulnerability in the framework's Jakarta Multipart parser. Hours later, an exploit for the flaw appeared on Chinese-language websites and this was almost immediately followed by real-world attacks, according to researchers from Cisco Systems.***
>
> ***The vulnerability is very easy to exploit and allows attackers to execute system commands with the privileges of the user running the web server process. If the web server is configured to run as root, the system is completely compromised, but executing code as a lower-privileged user is also a serious security threat.***
>
> ***What's even worse is that the Java web application doesn't even need to implement file upload functionality via the Jakarta Multipart parser in order to be vulnerable. According to researchers from Qualys, the simple presence***

> ***on the web server of this component, which is part of the Apache Struts framework by default, is enough to allow exploitation.***
>
> "Needless to say we think this is a high priority issue and the consequence of a successful attack is dire," said Amol Sarwate, director of Vulnerability Labs at Qualys, in a blog post.
>
> Companies who use Apache Struts on their servers should upgrade the framework to versions 2.3.32 or 2.5.10.1 as soon as possible.
>
> Researchers from Cisco Talos have observed "a high number of exploitation events." Some of them only execute the Linux command whoami to determine the privileges of the web server user and are probably used for initial probing. Others go further and stop the Linux firewall and then download an ELF executable that's executed on the server.
>
> "The payloads have varied but include an IRC bouncer, a DoS bot, and a sample related to the bill gates botnet," the Talos researchers said in a blog post.
>
> According to researchers from Spanish outfit Hack Players, Google searches indicate 35 million web applications that accept "filetype:action" uploads and a high percentage of them are likely vulnerable.
>
> It's somewhat unusual that attacks have started so quickly after the flaw was announced and it's not yet clear whether an exploit for the vulnerability already existed in closed circles before Monday.
>
> Users who can't immediately upgrade to the patched Struts versions can apply a workaround that consists of creating a Servlet filter for Content-Type that would discard any requests not matching multipart/form-data. Web application firewall rules to block such requests are also available from various vendors.[7]

(Emphasis added.) In plain English: the vulnerability allows a hacker easy access into Equifax's web servers and, once there, a hacker can run their own programs that can gain access to highly restricted data.

42. The vulnerability could have been fixed with relative ease with a software patch that was available on March 10, 2017. Typically, vulnerabilities are publicized only after solutions have been found, and this was the case with the Apache Struts vulnerability. In a

[7] https://www.pcworld.com/article/3178660/security/hackers-exploit-apache-struts-vulnerability-to-compromise-corporate-web-servers.html (last visited Nov. 17, 2017).

September 14, 2017, article on Wired.com titled "Equifax Officially Has No Excuse," tech reporter Lily Hay Newman explained:

> CAPPING A WEEK of incompetence, failures, and general shady behavior in responding to its massive data breach, Equifax has confirmed that attackers entered its system in mid-May through a web-application vulnerability that had a patch available in March. In other words, the credit-reporting giant had more than two months to take precautions that would have defended the personal data of 143 million people from being exposed. It didn't.
>
> A 'Relatively Easy' Hack
>
> The vulnerability that attackers exploited to access Equifax's system was in the Apache Struts web-application software, a widely used enterprise platform. The Apache Software Foundation said in a statement on Saturday (when rumors swirled that the March Struts bug might be to blame) that, though it was sorry if attackers exploited a bug in its software to breach Equifax, it always recommends that users regularly patch and update their Apache Struts platforms. "Most breaches we become aware of are caused by failure to update software components that are known to be vulnerable for months or even years," René Gielen, the vice president of Apache Struts, wrote.
>
> In this case, Equifax had ample opportunity to update.
>
> **"This vulnerability was disclosed back in March. There were clear and simple instructions of how to remedy the situation. The responsibility is then on companies to have procedures in place to follow such advice promptly," says Bas van Schaik, a product manager and researcher at Semmle, an analytics security firm. "The fact that Equifax was subsequently attacked in May means that Equifax did not follow that advice. Had they done so this breach would not have occurred."**

Emphasis added.[8]

43. Equifax CEO and Chairman, Richard F. Smith, announced his retirement on September 26, 2017. A week later, on October 2, 2017, Smith testified before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer

[8] https://www.wired.com/story/equifax-breach-no-excuse/

Protection. In prepared remarks, Smith testified that Equifax was specifically warned about the Apache Struts vulnerability on March 8, 2017, with an internal memo that was issued to patch the vulnerability, but that this was not done:

> First and foremost, I want to respond to the question that is on everyone's mind, which is, "How did this happen?" In my testimony, I will address both what I learned and did at key times in my role as CEO, and what I have since learned was occurring during those times, based on the company's ongoing investigation. Chronologically, the key events are as follows:
>
> On March 8, 2017, the U.S. Department of Homeland Security, Computer Emergency Readiness Team ("U.S. CERT") sent Equifax and many others a notice of the need to patch a particular vulnerability in certain versions of software used by other businesses. Equifax used that software, which is called "Apache Struts," in its online disputes portal, a website where consumers can dispute items on their credit reports.
>
> On March 9, Equifax disseminated the U.S. CERT notification internally by email requesting that applicable personnel responsible for an Apache Struts installation upgrade their software. Consistent with Equifax's patching policy, the Equifax security department required that patching occur within a 48 hour time period. We now know that the vulnerable version of Apache Struts within Equifax was not identified or patched in response to the internal March 9 notification to information technology personnel.
>
> On March 15, Equifax's information security department also ran scans that should have identified any systems that were vulnerable to the Apache Struts issue identified by U.S. CERT. Unfortunately, however, the scans did not identify the Apache Struts vulnerability. Equifax's efforts undertaken in March 2017 did not identify any versions of Apache Struts that were subject to this vulnerability, and the vulnerability remained in an Equifax web application much longer than it should have. I understand that Equifax's investigation into these issues is ongoing. The company knows, however, that it was this unpatched vulnerability that allowed hackers to access personal identifying information.

D. <u>Plaintiff Has Been Damaged By the Data Breach.</u>

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

45. Plaintiffs have 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.

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

47. Moreover, Plaintiffs have a continuing interest in ensuring that their private information, which remains in the possession of Equifax, is protected and safeguarded from future breaches.

48. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] 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."[10] As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[11]

49. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[12]

50. 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

[9] 17 C.F.R § 248.201 (2013).
[10] *Id.*
[11] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Nov. 17, 2017).
[12] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited Nov. 17, 2017).

average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[13]

51. 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:

> [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.[14]

52. Plaintiffs 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.

53. The Equifax Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiffs' 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 Plaintiffs' and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

54. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate,

---

[13] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Nov. 17, 2017).

[14] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited Nov. 17, 2017).

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.

55. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' 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, the 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.

56. 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 Plaintiffs and Class members, are ascertainable and are a determination appropriate for the trier of fact. Equifax has also not offered to cover any of the damages sustained by Plaintiffs or Class members.

57. While the PII of Plaintiffs and members of the Class has been stolen, Equifax continues to hold PII of consumers, including Plaintiffs and Class members. Particularly because Equifax has demonstrated an inability to prevent a breach, Plaintiffs 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.

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

58. 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.[15]

59. 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 one free year (an inadequately short amount) of credit monitoring and identity protection services.

60. 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 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 Nov. 17, 2017)

CLASS ALLEGATIONS

61. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seek 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").

[15] *Equifax Breach Response Turns Dumpster Fire*, https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/ (last visited Nov. 17, 2017).

62. 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 on behalf of citizens of those states, respectively, and on behalf of separate statewide classes, defined as follows:

> All persons residing in [STATE] whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017 (the "Statewide Classes"). 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.

63. Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

64. 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).

65. **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 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.

66. **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 Plaintiffs and Class members;

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

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

67. **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' PII was compromised in the Data Breach. Plaintiffs' damages and injuries are akin to other Class members and Plaintiffs seek relief consistent with the relief of the Class.

68. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are an adequate representative 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.

69. **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.

70. **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.

71. 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 Plaintiffs 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 Plaintiffs 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.

72. 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 Plaintiffs And The Nationwide Class, or Alternatively, on Behalf of PlaintiffsAnd The Statewide Classes

73. Plaintiffs restate and reallege Paragraphs 1 through 61 as if fully set forth herein.

74. Upon accepting and storing the PII 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 PII was private and confidential and should be protected as private and confidential.

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

76. 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 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.

77. Equifax had a special relationship with Plaintiffs 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.

78. Equifax's conduct also created a foreseeable risk of harm to Plaintiffs 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.

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

80. The law further imposes an affirmative duty on Equifax to timely disclose the unauthorized access and theft of the PII 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 PII.

81. 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.

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

83. 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 PII of Plaintiffs 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 Plaintiffs 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 Plaintiffs' and Class members' PII had been improperly acquired or accessed.

84. Equifax breached its duty to notify Plaintiffs and Class members of the unauthorized access by waiting six weeks after learning of the Data Breach to notify Plaintiffs and Class members of the Data Breach. 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 Plaintiff and the Class.

85. 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 bank accounts.

86. 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 Plaintiffs and Class members; and failing to provide Plaintiffs and Class members with timely and sufficient notice that their sensitive PII had been compromised.

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

88. As a direct and proximate cause of Equifax's conduct, Plaintiffs 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 Plaintiffs and Class members; damages arising from Plaintiffs' 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 Plaintiffs And The Nationwide Class, Or, Alternatively, Plaintiffs And The Statewide Classes)

89. Plaintiffs restate and reallege Paragraphs 1 through 89 as if fully set forth herein.

90. 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.

91. 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 Plaintiffs and Class members.

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

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

94. 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 Plaintiffs and the Class.

95. As a direct and proximate result of Equifax's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries arising from Plaintiffs' 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 Plaintiffs And The Nationwide Class)

96. Plaintiffs restate and reallege Paragraphs 1 through 94 as if fully set forth herein.

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

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

99. Plaintiffs and Class members entrusted Equifax with their PII.

100. 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 Plaintiffs 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.

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

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

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

104. Also as a direct result of Equifax's knowing violation of the GFBPA, Plaintiffs 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.

105. Plaintiffs bring this action on behalf of themselves and Class members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs 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.

106. Plaintiffs 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 Plaintiffs And The Nationwide Class)

107. Plaintiffs restate and reallege Paragraphs 1 through 105 as if fully set forth herein.

108. 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.

109. 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.

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

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

112. Had Equifax provided timely and accurate notice, Plaintiffs 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.

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

114. Plaintiffs 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, and reasonable attorney fees and costs, as provided by the applicable laws.

COUNT V
FAILURE TO TIMELY DISCLOSE BREACH UNDER MICH. COMP. LAWS ANN. 445.72(1)

(On Behalf Of The Michigan Class)

115. Plaintiffs restate and reallege Paragraphs 1 through 105 as if fully set forth herein.

116. Equifax is required to accurately notify the Class if it discovers a security breach, or receive notice of a security breach without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

117. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Mich. Comp. Laws Ann. § 445.72(1).

118. The Class' PII accessed in the Data Breached includes personal information as covered under Mich. Comp. Laws Ann. § 445.72(1).

119. Because Equifax discovered a security breach, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4). In mid-May 2017, Equifax's computer system storing personal and financial information was breached, and unauthorized individuals gained access to the information.

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

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

COUNT VI
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT,
CAL. CIV. CODE § 1798.80, et. seq.

(On Behalf of the California Class)

122. Plaintiffs restate and reallege Paragraphs 1 through 105 as if fully set forth herein.

123. Defendant is a business that owns, maintains, and licenses personal information, within the meaning of 1798.81.5, about Plaintiffs and Class Members.

124. Defendant violated Civil Code section 1798.81.5 by failing to implement reasonable measures to consumer PII.

125. Defendant is a businesses that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82.

126. The personal information Equifax has admitted was taken in the breach (social security numbers, etc…) constitutes personal information as covered by Cal. Civ. Code § 1798.82.

127. Because Equifax reasonably believed that PII was acquired by unauthorized persons during the Data Breach, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82, which it did not do.

128. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §§1798.81.5; 1798.82, the Class suffered damages, as described above.

COUNT VIIVIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW CAL. BUS. & PROF. CODE § 17200 — UNLAWFUL BUSINESS PRACTICES

(On Behalf of the California Class)

129. Plaintiffs repeat and fully incorporate the allegations contained in Paragraphs 1 through 61.

130. Defendants have violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200. Defendants engaged in unlawful acts and practices with respect to their services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Class Members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code §

1798.81.5, which required Defendants to use reasonable methods of safeguarding the PII of Plaintiffs and the Class Members.

131. In addition, Defendants engaged in unlawful acts and practices with respect to their services by failing to discover and then disclose the Data Breaches to Plaintiffs and Class Members in a timely and accurate manner so that they could take action to protect themselves from identity theft, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To date, Defendants have still not provided sufficient information to Plaintiffs and the Class Members.

132. As a direct and proximate result of Defendants' unlawful acts and practices, Plaintiffs and the Class Members were injured and lost money or property, including, but not limited to, the loss of their legally protected interest in the confidentiality and privacy of their PII, plus additional losses described above.

133. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data breach or theft was high. Defendants' actions and omissions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Class Members.

134. The members of the Class seek relief under Cal. Bus. & Prof. Code § 17200, *et. seq.*, including, but not limited to, restitution to Plaintiffs and Class Members of money or property that Defendants acquired by means of their unlawful and unfair business practices (including the monthly fees Defendants collected from Plaintiffs and the Class), restitutionary disgorgement of all profits accruing to Defendants because of their unlawful and unfair business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT VIII
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT RCW 19.86.010 *ET SEQ*On Behalf Of The Washington Class)

135. Plaintiffs restate and reallege Paragraphs 1 through 105 as if fully set forth herein.

136. The conduct of Defendant as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to accepting and storing Plaintiffs' 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.

137. Equifax also violated the Washington Consumer Protection Act by failing to immediately notify Plaintiffs and the Class of the Data Breach. If Plaintiffs 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.

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

139. 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).

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

141. 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*.

142. 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 Plaintiffs in this case were harmed, and many consumers were affected.

143. As a direct and proximate result of Equifax's negligence and misconduct described in this complaint, Plaintiffs 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.

144. Defendant's conduct proximately caused Plaintiffs' and the Class members' injuries.

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

COUNT IX
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT ("FCRA")

(On Behalf Of Plaintiffs And The Nationwide Class, Or, Alternatively, Plaintiffs And The Separate Statewide Classes)

145. Plaintiffs restate and reallege Paragraphs 1 through 144 as if fully set forth here.

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

147. 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.

148. 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).

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

150. 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' PII.

151. 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.

152. 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.

153. 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.

154. 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).

155. 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 X
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

(On Behalf Of Plaintiffs And The Nationwide Class, Or, Alternatively, Plaintiffs And The Separate Statewide Classes)

156. Plaintiffs restate and reallege Paragraphs 1 through 155 as if fully set forth herein.

157. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

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

159. Plaintiffs and the Nationwide Class members have been damaged by Equifax's negligent 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." 15 U.S.C. § 1681o(a)(1).

160. Plaintiffs and the Nationwide Class members are also entitled to recover their

costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, 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 Plaintiffs and their Counsel to represent the Nationwide Class, or in the alternative the separate State Classes;

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

c. For equitable relief compelling Equifax from delete all the information concerning class members in its possession and to discontinue collecting information about them;

d. 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;

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

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

g. For prejudgment interest on all amounts awarded; and

h. 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 28 day of November, 2017.

Respectfully submitted,

/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
Andrei V. Rado
Henry Kelston
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

LACKEY HERSHMAN, L.L.P.
Roger L. Mandel
3102 Oak Lawn Avenue, Suite 777
Dallas, Texas 75219-4259

Telephone: (214) 560-2201
Telecopier: (214) 560-2203

Counsel for Plaintiffs and the Proposed Class

CIVIL COVER SHEET

The JS 44 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, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Kurtis St. Clair, Kyle McClure, Jeremiah Smith, Courtney D. Smith, Josh Rupnow, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
James M. Evangelista, David J. Worley, Kristi Stahnke McGregor
EVANGELISTA WORLEY, LLC, 8100A Roswell Rd., Ste. 100, Atlanta, GA 30305, (404) 205-8400

DEFENDANTS

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.

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)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 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
- ☐ 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

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. 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)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(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 prote
Brief description of cause:

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P. **DEMAND $** CHECK YES only if demanded in complaint: **JURY DEMAND:** ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 11/28/2017

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

EXHIBIT A

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2017-5638 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the informatio

Current Description

The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generatior Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.

Source: MITRE **Last Modified:** 09/22/2017 ✚ View Analysis Description

QUICK INFO

CVE Dictionary Entry:
CVE-2017-5638

Original release date:
03/10/2017

Last revised:
11/09/2017

Source:
US-CERT/NIST

Impact

CVSS Severity (version 3.0):

CVSS v3 Base Score:
10.0 Critical

Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (legend)

Impact Score:
6.0

Exploitability Score:
3.9

CVSS Version 3 Metrics:

Attack Vector (AV):
Network

Attack Complexity (AC):
Low

Privileges Required (PR):
None

User Interaction (UI):
None

Scope (S):
Changed

Confidentiality (C):
High

Integrity (I):
High

Availability (A):
High

CVSS Severity (version 2.0):

CVSS v2 Base Score:
10.0 HIGH

Vector:
(AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore:
10.0

Exploitability Subscore:
10.0

CVSS Version 2 Metrics:

Access Vector:
Network exploitable

Access Complexity:
Low

Authentication:
Not required to exploit

Impact Type:
Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource	Type
http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html	Technical Description; Third Party Advisory	External S
http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/	Technical Description; Third Party Advisory	External S
http://www.eweek.com/security/apache-struts-vulnerability-under-attack.html	Press/Media Coverage	External S
http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html		External S
http://www.securityfocus.com/bid/96729	Third Party Advisory; VDB Entry	External S
http://www.securitytracker.com/id/1037973		External S
https://arstechnica.com/security/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/	Press/Media Coverage	External S
https://cwiki.apache.org/confluence/display/WW/S2-045	Mitigation; Vendor Advisory	External S
https://cwiki.apache.org/confluence/display/WW/S2-046		External S
https://exploit-db.com/exploits/41570	Exploit; VDB Entry	External S
https://git1-us-west.apache.org/repos/asf?p=struts.git;a=commit;h=352306493971e7d5a756d61780d57a76eb1f519a	Patch	External S
https://git1-us-west.apache.org/repos/asf?p=struts.git;a=commit;h=6b8272ce47160036ed120a48345d9aa884477228	Patch	External S
https://github.com/mazen160/struts-pwn	Exploit	External S

Hyperlink	Resource	Type
https://github.com/rapid7/metasploit-framework/issues/8064	Exploit	External S
https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03733en_us		External S
https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03749en_us		External S
https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03723en_us		External S
https://isc.sans.edu/diary/22169	Technical Description; Third Party Advisory	External S
https://nmap.org/nsedoc/scripts/http-vuln-cve2017-5638.html	Third Party Advisory	External S
https://packetstormsecurity.com/files/141494/S2-45-poc.py.txt	Exploit; VDB Entry	External S
https://security.netapp.com/advisory/ntap-20170310-0001/		External S
https://struts.apache.org/docs/s2-045.html		External S
https://struts.apache.org/docs/s2-046.html		External S
https://support.lenovo.com/us/en/product_security/len-14200		External S
https://twitter.com/theog150/status/841146956135124993	Third Party Advisory	External S
https://www.exploit-db.com/exploits/41614/		External S
https://www.imperva.com/blog/2017/03/cve-2017-5638-new-remote-code-execution-rce-vulnerability-in-apache-struts-2/		External S
https://www.kb.cert.org/vuls/id/834067		External S
https://www.symantec.com/security-center/network-protection-security-advisories/SA145		External S

Technical Details

Vulnerability Type (View All)

- Input Validation (CWE-20)

Vulnerable software and versions Switch to CPE 2.2

✚ Configuration 1

✚ OR

- ✱ cpe:2.3:a:apache:struts:2.3.5:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.6:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.7:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.8:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.9:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.10:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.11:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.12:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.13:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.14:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.14.1:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.14.2:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.14.3:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.15:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.15.1:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.15.2:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.15.3:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.16:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.16.1:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.16.2:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.16.3:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.17:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.19:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.20:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.20.1:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.20.2:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.20.3:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.21:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.22:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.23:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.24:*:*:*:*:*:*:*

- ✱ cpe:2.3:a:apache:struts:2.3.24.1:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.24.2:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.24.3:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.25:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.26:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.27:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.28:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.28.1:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.29:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.30:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.3.31:*:*:*:*:*:*:*

✚ **Configuration 2**

✚ OR

- ✱ cpe:2.3:a:apache:struts:2.5:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.5.1:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.5.2:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.5.3:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.5.4:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.5.5:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.5.6:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.5.7:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.5.8:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.5.9:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:apache:struts:2.5.10:*:*:*:*:*:*:*

✱ Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

Change History 16 change records found - show changes

HEADQUARTERS
100 Bureau Drive
Gaithersburg, MD 20899