Rosemary M. Rivas (State Bar No. 209147)
Email: rrivas@zlk.com
Quentin A. Roberts (State Bar No. 306687)
Email: qroberts@zlk.com
LEVI & KORSINSKY, LLP
44 Montgomery Street, Suite 650
San Francisco, California 94104
Telephone: (415) 291-2420
Facsimile: (415) 484-1294

Counsel for Plaintiffs Maria Schifano, LA' Sohn Smith, Dr. Heather Waitman, and Bob Helton

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

MARIA SCHIFANO, LA' SOHN SMITH, HEATHER WAITMAN, and BOB HELTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

EQUIFAX INC., a Georgia corporation,

Defendant.

Case No. 2:17-cv-6996

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Maria Schifano, LA' Sohn Smith, Dr. Heather Waitman, and Bob Helton (collectively, "Plaintiffs") individually and on behalf of the classes defined below, bring this Class Action Complaint ("Complaint") against Equifax Inc. ("Equifax" or "Defendant"), and allege as follows based on their personal experience and the investigation of their counsel:

NATURE OF THE CASE

1. On September 7, 2017, Equifax announced a massive nationwide data breach affecting nearly half of the United States population, an estimated 143 million Americans (the "Data Breach"). According to Equifax's limited press releases, unauthorized "criminals" accessed and stole the most sensitive personal information of consumers that was maintained on Equifax's servers. This information included

Social Security numbers, birthdates, address histories, legal names, and driver's license numbers (collectively, "PII"). This type of information is considered the "crown jewels of personal information" as it cannot be changed—once the PII is on the black market, it is there forever.

2. Equifax's response, to what is undeniably one of the worst data breaches in history, has angered nearly everyone. Aside from the fact that the company has not disclosed who stole the information, the agency apologized on Twitter saying, "Once discovered, we acted immediately to stop the intrusion." This statement, however, only added fuel to the fire as Equifax waited approximately six weeks to notify the public. The company stated the Data Breach occurred between mid-May and July of 2017, and Equifax allegedly discovered the hack on July 29, 2017.

3. On information and belief, in March 2017, approximately two months before the Data Breach occurred, cybersecurity professionals discovered a coding flaw in Apache Struts, an open source software in which the hack occurred, and shared a fix for it with an industry group, making it available to any company that uses the software, such as Equifax. Disturbingly, rather than implement the patch to fix the vulnerability, Equifax failed to install the security updates. This known but ignored vulnerability directly led to the Data Breach.

4. The Data Breach occurred not only because Equifax failed to implement adequate security measures to safeguard consumers' PII, but because it ignored *known* weaknesses in its data security system. Weaknesses that were communicated approximately two months before the Data Breach. Moreover, hackers routinely attempt to gain access to and steal personal information from networks and information systems—especially from entities such as Equifax known to possess a large number of individuals' valuable personal and financial information.

5. Once cybercriminals obtain PII, thieves can commit a variety of crimes

that harm victims of the Data Breach. For example, they can take out loans, mortgage property, open financial accounts, open credit cards in a victim's name, use a victim's information to obtain government benefits, obtain student loans, obtain medical care, buy drugs, file fraudulent returns to obtain a tax refund, obtain a driver's license or identification card in a victim's name, gain employment in another person's name, or give false information to police during an arrest. Hackers also routinely sell individuals' PII to other individuals who intend to misuse the information.

6. Due to Equifax's willful failure to prevent the Data Breach, Plaintiffs and Class Members have been exposed to fraud, identity theft, and financial harm, as detailed below, and are at a heightened, imminent risk of such harm in the future, possibly lasting a lifetime. Plaintiffs and Class Members are now required to closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and likely will have to incur additional, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to detect and address identity theft.

7. Plaintiffs bring this action to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was compromised during the Data Breach. Plaintiffs seek the following remedies, among other things: reimbursement of out-of-pocket losses, other compensatory damages, further credit monitoring services with accompanying identity theft insurance beyond Equifax's current one-year offer, and injunctive relief, including an order requiring Equifax to implement improved data security measures that comport with industry standards so that another data breach does not reoccur.

PARTIES

8. Plaintiff Bob Helton is a resident of Calvert City, Kentucky and was a Kentucky resident during the Data Breach. Mr. Helton has suffered identity theft and is at a heightened risk of suffering further identity theft in the future, particularly

because his Social Security number, among other extremely sensitive PII, was stolen as a result of the Data Breach. On or around August 16, 2017, Mr. Helton discovered that an unauthorized criminal had cancelled his credit card and had a new credit card issued to a different address. Over $11,000 was fraudulently charged to Mr. Helton's credit card. Mr. Helton promptly informed his bank of the fraudulent activity and had that card cancelled. However, the identity thieves had his bank fraudulently issue new credit cards *two more times* within the span of several days. The bank later informed Mr. Helton that the impersonator who called provided, at a minimum, Mr. Helton's Social Security number, driver's license number, address, and legal name. After the third credit card was fraudulently issued, Mr. Helton had a freeze placed on that account and filed a police report. Mr. Helton must now regularly monitor his banking and credit information as well as his accounts in order to determine whether any additional fraudulent or unauthorized activity has taken place due to the compromise of his information. If a criminal does attempt to further fraudulently use Mr. Helton's information in the future, as with the other Plaintiffs, he will have to spend time and money in protecting his information and taking any corrective actions. In particular, he may have to take additional time off from work in order to travel to an IRS office to personally verify his identity for tax purposes. As a result of the Data Breach, Mr. Helton signed up for Lifelock and is paying approximately $29.95 per month for its monitoring service. Additionally, Mr. Helton had to miss approximately 30 hours of work to address the fraudulent activity, resulting in 30 hours of lost wages. Mr. Helton's wife has also had to spend approximately seven hours in dealing with the repercussions of the Data Breach.

9. Plaintiff LA' Sohn Smith is a resident of Randallstown, Maryland and was a Maryland resident during the Data Breach. Ms. Smith has suffered identity theft and is at a heightened risk of suffering further identity theft in the future, particularly because her Social Security number, among other extremely sensitive PII, was stolen as a result of the Data Breach. Ms. Smith received an email in

August of 2017 from Lending Tree informing her that a loan she applied for could not be approved. Ms. Smith, however, did not apply for a loan. This was a fraudulent attempt at identity theft because of the Data Breach. Additionally, in September of 2017, Ms. Smith incurred approximately four fraudulent charges to Dunkin Donuts on her credit card that she did not make nor authorize. Ms. Smith must now regularly monitor her banking and credit information as well as her accounts in order to determine whether any additional fraudulent or unauthorized activity has taken place due to the compromise of her information. If a criminal does attempt to further fraudulently use Ms. Smith's information in the future, as with the other Plaintiffs, she will have to spend additional time and money in protecting her information and taking any corrective actions. In particular, she may have to take time off from work in order to travel to an IRS office to personally verify her identity for tax purposes. Additionally, since 2016, Ms. Smith has been paying approximately $20 a month for Equifax's credit monitoring service. Ms. Smith is now considering paying for extra credit monitoring. As a result of the Data Breach, Ms. Smith has spent approximately five hours addressing issues arising from the Data Breach, including checking her accounts and credit report for fraud.

10. Plaintiff Maria Schifano is a resident of Las Vegas, Nevada and was a Nevada resident during the Data Breach. Ms. Schifano is at a heightened risk of suffering identity theft in the future, particularly because her Social Security number, among other extremely sensitive PII was stolen as a result of the Data Breach. Ms. Schifano must now regularly monitor her banking and credit information as well as her accounts in order to determine whether any fraudulent or unauthorized activity has taken place due to the compromise of his information. If a criminal does attempt to fraudulently use Ms. Schifano's information in the future, as with the other Plaintiffs, she will have to spend additional time and money in protecting her information and taking any corrective actions. In particular, she may have to take time off from work in order to travel to an IRS office to personally verify her identity

for tax purposes. As a result of the Data Breach, Ms. Schifano has enrolled in Lifelock to monitor her accounts for approximately $270 per year. Additionally, for the last three years, Ms. Schifano has paid Equifax approximately $20 a month to monitor her accounts. Ms. Schifano is a business owner and is now required to spend approximately one hour each day monitoring her accounts and credit report for instances of identity theft or fraudulent activity.

11. Plaintiff Dr. Heather Waitman is a resident of Pearl River, New York and was a New York resident during the Data Breach. Dr. Waitman has suffered identity theft and is at a heightened risk of suffering further identity theft in the future, particularly because her Social Security number, among other extremely sensitive PII, was stolen as a result of the Data Breach. Dr. Waitman received an email in early August of 2017 from her bank, Chase, asking her to confirm that she spent approximately $1,113.75 at Barneys New York, a clothing store, located in Beverly Hills, California. Dr. Waitman informed her bank that this was a fraudulent charge and that she is in New York, not California. Moreover, this fraudulent charge was made with her debit card and exhausted the funds in her checking account linked to that debit card. Dr. Waitman later called her bank to find out if any additional fraudulent activity had taken place. To her dismay, a Chase representative informed her that someone called to transfer $2,500 from her savings account to the checking account linked to her debit card. Dr. Waitman again informed her bank that this was fraudulent and asked them to close her accounts with the bank. Before the accounts could be closed, someone fraudulently transferred a second amount of $2,500 from her savings account to her checking account. Additionally, Dr. Waitman was told that the person impersonating her changed the home phone number associated with her account. Dr. Waitman filed a police report. Dr. Waitman must now regularly monitor her banking and credit information as well as her accounts in order to determine whether any additional fraudulent or unauthorized activity has taken place due to the compromise of her information. If a criminal does attempt to further

fraudulently use Dr. Waitman's information in the future, as with the other Plaintiffs, she will have to spend additional time and money in protecting her information and taking any corrective actions. In particular, she may have to take additional time off from work in order to travel to an IRS office to personally verify her identity for tax purposes. Dr. Waitman is also considering paying extra for credit monitoring. As a result of the Data Breach, Dr. Waitman has spent approximately 20 hours addressing issues arising from the Data Breach, including checking her accounts and credit report for fraud. Additionally, Dr. Waitman had to take time off from work four days in a row to resolve the fraudulent activity at her bank.

12. Defendant Equifax Inc. is incorporated in Georgia, with its corporate headquarters located at 1550 Peachtree Street NE, Atlanta, GA 30309. It is a citizen of Georgia.

13. Equifax is one of the three largest American consumer reporting agencies in the United States. It gathers and maintains information on over 800 million consumers and more than 88 million businesses worldwide. In 2016, its revenue exceeded $3.14 billion. It is listed on the New York Stock Exchange.

14. As a reporting agency, Equifax is engaged in a number of credit-related services, including assisting organizations with evaluating the risks and rewards associated with providing credit to consumers and businesses and providing people with online access to their credit history and score. As a consumer reporting agency, Equifax maintains information related to the credit history of consumers and provides the information to credit grantors who are considering a borrower's application for credit or who have extended credit to the borrower.

JURISDICTION AND VENUE

15. This Court has diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 Class Members, the amount in controversy exceeds $5 million exclusive of interest and costs, and many members of the Class are citizens of states different

from Defendant.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Equifax regularly transacts business here, and thousands of the Class Members reside in this District. In addition, the events giving rise to Plaintiffs' causes of action arose, in part, in this District.

FACTUAL ALLEGATIONS

A. Equifax and Its Wealth of Sensitive Consumer Data

17. Equifax and two other consumer reporting bureaus, Experian and TransUnion, create credit files on consumers used to calculate consumer credit scores. The three-digit credit score is what banks, insurers, lenders, and employers rely on to make many important decisions for consumers, ranging from getting a new job to securing a home loan.

18. The reality is that many consumers have no choice as to whether Equifax should possess their sensitive and confidential PII because banks and other companies hand over financial information and other data directly to credit bureaus, including Equifax.

19. Despite the wealth of extremely sensitive information Equifax stores, it does not have the constant monitoring and auditing that banks' systems have to maintain data protection. Unfortunately, the oversight for these bureaus is much more lax than the oversight of banks. Moreover, because of Equifax's willful disregard for maintaining sufficient data security systems on par with the industry standard, cybercriminals stole the sensitive PII and consumers are paying the price.

20. Financial experts believe the Data Breach will leave millions of Americans at risk of identity theft *for the rest of their lives*.

B. The Data Breach and How It Happened

21. On September 7, 2017, Equifax disclosed the Data Breach to the public. It admitted that the breach compromised the PII of 143 million Americans, or about half of the nation. According to Equifax, unauthorized cybercriminals acquired the

highly sensitive PII from Equifax's servers. The PII included Social Security numbers, birthdates, address histories, legal names, driver's license numbers, and/or credit card numbers.

22. On September 12, 2017, Equifax stated that the Data Breach was due to an Apache Struts vulnerability. Apache Struts is a free, open-source software that is used to create Java web applications. Equifax claims that several vulnerabilities have been patched, however, it would not disclose which one was responsible for the Data Breach.

23. Security experts note that aside from the particular vulnerability that led to the Data Breach, Equifax should have had security controls in place that would have precluded such a catastrophic outcome from happening. For example, it is unclear if Equifax used a standard security technique of segmenting networks so that even if hackers were able to infiltrate the company's system, they would only be able to access a limited amount of data.

24. Another common question circulating among data security experts is how the cybercriminals obtained all of that data without anyone within Equifax's security group noticing. The PII of 143 million Americans is not a small data load. Itzik Kotler, Chief Technology Officer at SafeBreach, a company that develops breach and remediation scenarios stated, "Someone should have said 'This server's load is incredibly high right now, what's going on?' What kind of business doesn't watch for that?"

25. Recent news suggests that not only did Equifax fail to have security systems in place to detect and stop the intrusion earlier, but the company willfully allowed the Data Breach to occur by ignoring a patch it had been provided two months before the hack happened.

C. Equifax Allowed the Data Breach to Happen

26. On September 14, 2017, a week after the Data Breach, the Apache Foundation, an industry group which oversees the widely-used open source

software, specifically blamed Equifax for the breach. It stated that "The Equifax data compromise was due to (Equifax's) failure to install the security updates provided in a timely manner."

27. On September 13, 2017, Equifax told USA TODAY that the cybercriminals exploited a website application vulnerability known as Apache Struts CVE-2017-5638. This is particularly disturbing as cybersecurity professionals who lend their free services to the project of open-source software, *shared this particular risk and fix* with the industry group, making the risk and fix known to any company using the software. According to the Nation Vulnerability Database, this was shared on March 10, 2017. This was *two months* before the Data Breach took place.

28. This patch should have been applied to Equifax's system within days. As a result of the recent developments, the Federal Trade Commission and the Consumer Financial Protection Bureau have stated they have initiated probes into this hack. Moreover, dozens of state attorneys general are investigating the Data Breach.

29. Equifax knew that its information security systems and practices were inadequate to prevent unauthorized users from accessing information housed in its servers and networks. Equifax had the tools and information to prevent the hack two months before it occurred, and yet it failed to do so.

D. Equifax's Response and Proposed Remedy

30. On September 12, 2017, Richard F. Smith, Chairman and Chief Executive Officer of Equifax, reported that the company first discovered the intrusion on July 29, 2017. Moreover, Smith also acknowledged the general outcry regarding the six-week delay in notifying the public that the most sensitive PII of 143 million Americans was stolen. His response was that the company thought the breach was more limited. Smith also encouraged the public to take advantage of Equifax's offered protection due to the Data Breach. As of September 12, 2017, approximately 11.5 million consumers have enrolled.

31. However, Equifax's offered remedial plan is grossly insufficient. First, it set up a website so consumers could determine if their PII was compromised in the Data Breach. In order to find out, consumers are required to enter the last six digits of their Social Security number along with their last name. Many consumers are wary to do so as this is the same company that just allowed the hack to occur. Aside from that, the website only offered vague responses saying personal information was not impacted or that it "may have been impacted." This does not provide meaningful notice. Additionally, some people found that entering fake names and numbers generated the same messages.

32. Initially, enrolling in Equifax's credit monitoring service required users to waive their rights to legal action and agree to exclusively use arbitration to settle any disputes. This immediately caused more outrage. Many prominent figures spoke out against this, including the New York Attorney General, Mr. Eric Schneiderman, who stated this language should be removed. Equifax later amended its Terms of Use to reflect that the arbitration clause would not apply to the Data Breach.

33. Currently, Equifax's solution is to offer one year of free credit monitoring to all consumers affected. It is also providing consumers the ability to lock their Equifax reports, which, in theory, should prevent thieves from applying for credit in their name. Poignantly, however, Adam Levin, Chairman of CyberScout, a company that provides data breach defense services, stated that "This is a one-year solution for an eternal problem."

34. One year of credit monitoring is woefully inadequate. A person is provided with one Social Security number for their life, and once that number is on the black market, it will remain there forever. One year of added monitoring only means that cybercriminals must simply wait one year before committing identity theft and all of the collateral damage that comes along with it. Importantly, credit monitoring typically does not prevent identity theft, it only alerts people once it has

already happened.

35. Additionally, the credit monitoring service Equifax is offering is its own product. Moreover, the company will likely make many millions of dollars off of the very victims of its own Data Breach considering some percentage of people affected are likely to pay for the monitoring once the free one-year service expires. At the current price of $19.95 a month, this would lead to revenue for Equifax of over $300 million if only one percent of the affected people signed up for one year of its pay-for service.

E. Equifax Suffered an Additional Hack Approximately Two Months Before the Data Breach that Compromised 143 Million Americans' PII

36. On September 18, 2017, it was reported that Equifax suffered an additional breach on its system in March of 2017, approximately two months before the Data Breach that compromised 143 million Americans. This was approximately five months before the company disclosed the later Data Breach to the public.

37. Equifax reportedly told Bloomberg that the March breach was not related to the massive Data Breach, however, one source familiar with the situations believes the breaches involved the same intruder(s).

38. Whether this is true or not, it raises the question as to whether Equifax should have been able to prevent, or at least better minimize the intrusion that took place in or around May of 2017. The answer is undeniably—yes.

39. Equifax reportedly hired the security firm Mandiant to investigate the March breach. Mandiant also has been involved in the investigation of the most recent Data Breach.

F. By Federal Regulation, Equifax Was Required to Investigate and Provide Timely and Adequate Notification of the Data Breach

40. The Gramm-Leach-Bliley Act ("GLBA") imposes upon "financial institutions" "an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers'

nonpublic personal information." 15 U.S.C. § 6801. To satisfy this obligation, financial institutions must satisfy certain standards relating to administrative, technical, and physical safeguards:

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

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

> (a) Designate an employee or employees to coordinate [their] information security program.
>
> (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of [their] operations, including:
>
> (1) Employee training and management;
>
> (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
>
> (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
>
> (c) Design and implement information safeguards to control the risks [they] identify through risk assessment, and regularly

> test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
>
> (d) Oversee service providers, by:
>
> (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
>
> (2) Requiring [their] service providers by contract to implement and maintain such safeguards.
>
> (e) Evaluate and adjust [their] information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to [their] operations or business arrangements; or any other circumstances that [they] know or have reason to know may have a material impact on [their] information security program."

Id.

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

> 1. At a *minimum*, an institution's response program should contain procedures for the following:
>
> a. Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;
>
> b. Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below;
>
> c. Consistent with the Agencies' Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;
>
> d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and

e. Notifying customers when warranted.

Id. (emphasis added).

43. Further, "[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible." *See id.*

44. Credit bureaus are "financial institutions" for purposes of the GLBA, and are therefore subject to its provisions. *See TransUnion LLC v. FTC*, 295 F.3d 42, 48 (D.C. Cir. 2002). Under Regulation Y promulgated by the Federal Reserve Board, *Bank Holding Companies and Change in Bank Control*, "credit bureau services[1]" are "so closely related to banking or managing or controlling banks as to be a proper incident thereto." 12 CFR Part 225.28. Because Equifax is a credit bureau and performs credit bureau services, it qualifies as a financial institution for purposes of the GLBA.

45. "Nonpublic personal information," includes PII (such as the PII compromised during the Data Breach) for purposes of the GLBA. Likewise, "sensitive customer information" includes PII for purposes of the Interagency Guidelines Establishing Information Security Standards.

46. Upon information and belief, Equifax failed to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.3. This includes, but is not

[1] Credit bureau services include "[m]aintaining information related to the credit history of consumers and providing the information to a credit grantor who is considering a borrower's application for credit or who has extended credit to the borrower." 12 C.F.R. § 225.28(b)(2)(v).

limited to, Equifax's (a) failure to implement and maintain adequate data security practices to safeguard Class Members' PII; (b) failure to detect the Data Breach in a timely manner; and (c) failure to disclose that its data security practices were inadequate to safeguard Class Members' PII.

47. Upon information and belief, Equifax also failed to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See* 16 C.F.R. § 314.3. This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

48. Upon information and belief, Equifax also failed to notify affected consumers in an appropriate timeframe as it waited approximately six weeks after it became aware of unauthorized access to sensitive consumer information.

CLASS ACTION ALLEGATIONS

49. Plaintiffs bring this action on behalf of themselves and the members of the proposed Classes under Rule 23(a), (b)(2), (b)(3), and/or (c)(4) of the Federal Rules of Civil Procedure.

A. Nationwide Class

50. Plaintiffs bring their negligence and negligence per se claims (Counts I and II) on behalf of a proposed nationwide class ("Nationwide Class"), defined as follows: **All natural persons and entities in the United States whose personal identifying information was acquired by unauthorized user(s) as announced by Equifax in September 2017.**

B. Multistate Class

51. In the alternative, Plaintiffs also bring their negligence and negligence per se claims (Counts I and II) on behalf of a multistate class ("Multistate Class") defined as follows: **All natural persons and entities residing in the states of Kentucky, Maryland, Nevada and New York whose personal identifying**

information was acquired by unauthorized user(s) as announced by Equifax in September 2017.

52. Except where otherwise noted, "Class Members" shall refer to members of the Nationwide Class and each of the Multistate Class, collectively.

53. Excluded from the Classes are Defendant, its parents, subsidiaries, affiliates, officers and directors, any entity in which Defendant has a controlling interest, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

54. Numerosity. Fed. R. Civ. P. 23(a)(1). The Nationwide and Multistate Classes are so numerous that joinder of all members is impracticable. According to Equifax itself, the Nationwide Class includes approximately 143 million individuals whose PII was acquired during the Data Breach. On information and belief, Plaintiffs allege that there are also at least thousands of individuals in the Multistate Class as well. The parties will be able to identify each member of the Nationwide and Multistate Classes after Defendant's document production and/or related discovery takes place.

55. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are numerous questions of law and fact common to Plaintiffs and the Nationwide and Multistate Classes, including but not limited to the following:

a. Whether Defendant engaged in the wrongful conduct alleged herein;
b. Whether Defendant owed a duty to Plaintiffs and Class Members to adequately protect their PII;
c. Whether Defendant breached its duties to protect the PII of Plaintiffs and Class Members;
d. Whether Defendant knew or should have known that its data security systems and processes were vulnerable to attack;
e. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's conduct, including increased risk of

identity theft and loss of value of PII;

f. Whether Defendant owed a duty to Plaintiffs and Class Members to inform them of the Data Breach sooner than six weeks after it was discovered;

g. Whether Defendant had a duty to implement the Apache Struts patch before the Data Breach occurred; and

h. Whether Plaintiffs and Class Members are entitled to equitable relief including injunctive relief.

56. Typicality. Fed. R. Civ. P. 23(a)(3). All Plaintiffs' claims are typical of the claims of the Nationwide Class, and each Plaintiff's claims is typical of the claims of the Multistate Class. Each of the Plaintiffs, like all proposed Class Members, had their PII compromised in the Data Breach.

57. Adequacy. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately protect the interests of the Nationwide and Multistate Classes. Plaintiffs have no interests that are adverse to, or in conflict with, the Class Members. There are no claims or defenses that are unique to Plaintiffs. Likewise, Plaintiffs have retained counsel experienced in class action and complex litigation, including data breach litigation, that have sufficient resources to prosecute this action vigorously.

58. Superiority. Fed. R. Civ. P. 23(b)(3). The proposed action also meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

59. Absent a class action, the majority of Class Members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

60. The prosecution of separate actions by members of the Class would

create a risk of establishing inconsistent rulings and/or incompatible standards of conduct for Defendant. Additionally, individual actions may be dispositive of the interests of the Class, although certain Class Members are not parties to such actions.

61. Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2). In addition, Defendant has acted and/or refused to act on grounds that apply generally to the Nationwide and Multistate Classes, making injunctive and/or declaratory relief appropriate with respect to the classes under Federal Rule of Civil Procedure 23(b)(2). Defendant continues to (1) maintain the PII of Class Members, and (2) fails to adequately protect their PII.

62. Issue Certification. Fed. R. Civ. P. 23(c)(4). In the alternative, the Nationwide and Multistate Classes may be maintained as class actions with respect to particular issues, as set forth in Paragraph 55.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On Behalf of the Nationwide Class and Multistate Class)

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

64. Equifax owed a duty to Plaintiffs and Class Members, arising from the highly sensitive nature of the information it possesses and the foreseeability of its data security shortcomings resulting in an intrusion and to exercise reasonable care in safeguarding their sensitive PII. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class Members' information was adequately secured from unauthorized access.

65. Equifax's privacy policy states it is committed to protecting the security of Class Members' PII and that it maintains "a highly sophisticated data information network that includes advanced security, protections and redundancies."

66. Equifax owed a duty to Class Members to implement intrusion detection processes that would detect a data breach in a timely manner.

67. Equifax also had a duty to delete any PII that was no longer needed to serve client needs.

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

69. Equifax owed a duty to disclose the material fact that Plaintiffs' and Class Members' PII was stolen in the Data Breach in a timely fashion such that Plaintiffs and Class Members could reasonably safeguard and take precautions against incurring further identity theft, identity fraud, and/or damages.

70. Equifax owed a duty to implement the Apache Struts patch after it was notified that there was an industry-wide vulnerability.

71. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class Members' PII; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that its data security practices were inadequate to safeguard Class Members' PII; (d) failing to disclose in a timely fashion to Plaintiffs and Class Members that their PII had been stolen through the Data Breach such that they could reasonably safeguard and take precautions against incurring further identity theft, identity fraud, and/or damages; and (e) failing to implement the Apache Struts vulnerability patch prior to the Data Breach.

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

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

74. Equifax's negligent conduct provided a means for unauthorized cybercriminals to obtain Plaintiffs' and Class Members' PII and consumer reports

for no permissible purposes.

75. As a result of Equifax's willful failure to prevent the breach, Plaintiffs and Class Members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must now closely monitor their financial accounts and credit histories to guard against identity theft or further identity theft. Class Members also have incurred, and likely will have to incur, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of the PII.

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

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

COUNT II

NEGLIGENCE PER SE

(On Behalf of the Nationwide Class and Multistate Class)

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

79. As detailed in Paragraphs 40-48, Equifax was required under the GLBA to satisfy certain standards relating to administrative, technical, and physical safeguards:

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

any customer.

80. In order to satisfy their obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.3.

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

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

83. Equifax violated GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.3. This includes, but is not limited to, Equifax's (a) failure to implement and maintain adequate data security practices to safeguard Class Members' PII; (b) failure to detect the Data Breach in a timely manner; (c) failure to disclose that Defendant's data security practices were inadequate to safeguard Class Members' PII; (d) failure to disclose in a timely fashion to Plaintiffs and Class Members that their PII had been stolen through the Data Breach such that they could reasonably safeguard and take precautions against

incurring further identity theft, identity fraud, and/or damages; and (e) failure to implement the Apache Struts vulnerability patch prior to the Data Breach.

84. Equifax also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to consumer information in consumer information systems." *See* 16 C.F.R. § 314.3. This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

85. Equifax also violated the GLBA by failing to notify affected consumers as soon as possible after it became aware of unauthorized access to sensitive customer information such that they could reasonably safeguard and take precautions against incurring further identity theft, identity fraud, and/or damages.

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

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

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

89. As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiffs and Class Members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and may have to incur, out-of-pocket costs for obtaining credit

reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' PII has also diminished the value of the PII.

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

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

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and all others similarly situated, request that the Court enter judgment against Equifax as follows:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Classes requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein;

B. Injunctive relief requiring Defendant to (1) strengthen its data security systems that maintain PII to comport with industry standards and comply with the GLBA; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendant's systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify, and contain a breach, and how to appropriately respond;

C. An order requiring Defendant to pay all costs associated with Class notice and administration of Class-wide relief;

D. An award to Plaintiffs and all Class Members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

E. An award to Plaintiffs and all Class Members of additional credit monitoring and identity theft protection services beyond the one-year package Equifax is currently offering;

F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An order requiring Defendant to pay pre-judgment and post-judgment interest, as provided by law or equity; and

F. Such other or further relief as the Court may allow.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all issues in this action so triable of right.

Dated: September 21, 2017

LEVI & KORSINSKY, LLP

By: /s/ *Rosemary M. Rivas*
Rosemary M. Rivas

Quentin A. Roberts
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 291-2420
Facsimile: (415) 484-1294

Counsel for Plaintiffs
Maria Schifano, LA' Sohn Smith,
Dr. Heather Waitman, and Bob Helton