ERIK S. SYVERSON (BAR NO. 221933)
esyverson@raineslaw.com
RAINES FELDMAN LLP
1800 Avenue of the Stars, 12th Floor
Los Angeles, California 90067
Telephone: (310) 440-4100
Facsimile: (310) 765-7730

Attorneys for Plaintiff Carson Block

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

CARSON BLOCK, an individual ;

Plaintiff,

v.

EQUIFAX, INC., a Georgia Corporation; RICHARD F. SMITH, an Individual, SUSAN MAULDIN, an Individual, MARY HANNAN, an Individual, GRAEME PAYNE, an Individual, HAROLD BOUTIN, an Individual, ROBERT FRIEDRICH, an Individual, VIDYA SAGAR JAGADAM, an Individual, LARA PEARSON, an Individual, SHEA GIESLER, an Individual, CLIFF BARBIER, an Individual, JOE SANDERS, an Individual, and DOES 1 through 25, inclusive;

Defendants.

Case No. 17-5367

COMPLAINT FOR:
(1) Negligence; and
(2) Violations of Unfair Competition Law (Cal. Bus. & Prof. Code § 17200, *et seq*.)

DEMAND FOR JURY TRIAL

Plaintiff Carson Block ("Block" or "Plaintiff") files this Complaint against Equifax, Inc. ("Equifax" or "the Company"), and responsible officers, employees, and agents thereof, including Richard F. Smith, the Chairman of the Board and Chief Executive Officer of Equifax, Susan Mauldin, the Chief Information Security Officer (CISO) at Equifax, Mary Hannan, the Senior Vice President, Corporate Technology Legal and Security Support at Equifax, Graeme Payne, the Vice President of IT Risk and Compliance at Equifax, Harold Boutin, the Senior Vice President - IT Strategy and Effectiveness at Equifax, Robert Friedrich, the SVP/CIO Global Consumer Solutions at Equifax, Vidya Sagar Jagadam, the Vice President, IT Governance, Risk & Compliance at Equifax, Lara Pearson, the Senior Director of Risk Security Programs at Equifax, Shea Giesler, the Vice President, Security Programs at Equifax, Cliff Barbier, the Director, Security Engineering Solutions at Equifax, Joe Sanders, an individual of residence unknown, was the Senior Director of Security Engineering Solutions at Equifax, and DOES 1 through 25, inclusive, and alleges the following based on personal knowledge, the investigation of counsel, and information and belief:

I. INTRODUCTION

1. Equifax is in the business of selling consumer credit and insurance reports and related analytics to businesses in a range of industries. As one of the three major credit reporting companies in the United States that collects and aggregates financially sensitive personally identifiable information ("PII"), Equifax is regularly entrusted with the storage, and security of PII. Equifax stores PII relating to over 800 million individual consumers and more than 88 million businesses worldwide. In the United States, the PII held by Equifax includes names, Social Security numbers, birth dates, driver's license numbers, and credit card numbers.

2. According to Equifax, on July 29, 2017, it discovered that "criminals exploited a U.S. website application vulnerability" ("the Vulnerability") in its

system to "gain access to certain files" "potentially impacting information relating to approximately 143 million U.S. consumers." (the "Data Breach"). The information accessed by the "criminals" "primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers," along with credit card numbers and dispute documents with other PII for a smaller subset of consumers.

3. In the period shortly after the discovery of the Data Breach, on July 29, 2017, and well before the public disclosure of the breach, Equifax managers sold shares worth almost $1.8 million.

4. It was not until 40 days after the Data Breach was discovered that Equifax finally made a limited public disclosure, admitting the scope of the breach via a press release and notifications to the Attorneys General of California and other States. Equifax decided to mail notices to the small percentage of consumers believed to have been affected by the credit card or dispute document disclosures, but not the 143 million or more that had their other PII had exposed to criminals. Instead, for those consumers, Equifax expected consumers to check for themselves on a poorly designed, unreliable, and potentially insecure website, www.equifaxsecurity2017.com.

5. As a result of the Data Breach, Block has suffered injuries stemming from an immediate and heightened risk of all manners of identity theft, including but not limited to:

a. Theft of their personal and financial information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of personal information and/or financial accounts;

c. Unauthorized debit and/or credit account charges;

d. Loss of use of and/or access to account funds and costs associated with inability to obtain money from accounts or being

limited in the amount of money they were permitted to obtain from their accounts, including consequential damages such as missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax data breach;

f. The imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet and/or black market; and

g. Damages to and diminution in value of personal and financial information held and exposed by Equifax.

6. Equifax was negligent in taking the necessary precautions required to safeguard and protect Plaintiff's PII from criminals, and also breached its duty to timely and adequately disclose the Data Breach.

7. Furthermore, Equifax is in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL") for failing to take reasonable measures in protecting Plaintiff's PII

II. THE PARTIES

8. Plaintiff Carson Block is an individual consumer and resident of San

Francisco County, California. On or about September 8, 2017, Block entered his information on equifaxsecurity2017.com and subsequently received a message from Equifax informing him that his PII had been stolen by cybercriminals in the Data Breach. As a result of the Data Breach Plaintiff has suffered a loss of privacy, is at a continuous high risk of identity theft or other types of financial fraud, and will continue to suffer from the increased financial and mental costs necessary to consistently monitor and guard against the aforementioned risks.

9. Equifax Inc. is a multi-billion dollar corporation, incorporated in Georgia, and headquartered in Atlanta, Georgia. Equifax operates through various subsidiaries including Equifax Information Services, LLC, and Equifax Consumer Services, LLC aka Equifax Personal Solutions aka PSOL. Each of these entities acted as agents of Equifax or in the alternative, acted in concert with Equifax as alleged in this complaint.

10. On information and belief, Richard F. Smith, an individual of residence unknown, was the Chairman of the Board and Chief Executive Officer of Equifax at the time of the Data Breach, where had had the responsibility for the operations of Equifax and failed to use his authority to strengthen Equifax's defenses against cybercrimes such as the Data Breach.

11. On information and belief, Susan Mauldin, an individual of residence unknown, was the Chief Information Security Officer (CISO) at Equifax at the time of the Data Breach. On information and belief, the CISO of Equifax was directly responsible for management of Equifax's employees or officers maintaining the confidentiality, availability, and integrity of Equifax's consumer data and the security of the assets of the company, such as the PII subject to the Data Breach.

12. On information and belief, Mary Hannan, an individual of residence unknown, was the Senior Vice President, Corporate Technology Legal and Security Support at Equifax at the time of the Data Breach. On information and belief, in this role at Equifax Ms. Hannan was the strategic leader responsible for IT tools support

and compliance in connection with legal and security business units and for oversight of hardware/software asset management.

13. On information and belief, Graeme Payne, an individual of residence unknown, was the Vice President of IT Risk and Compliance at Equifax at the time of the Data Breach. On information and belief, in this role at Equifax Mr. Payne was Responsible for leading initiatives around IT risk and compliance, including access management, IT risks and controls, regulatory compliance, asset management, software compliance and contracts

14. On information and belief, Harold Boutin, an individual of residence unknown, was the Senior Vice President - IT Strategy and Effectiveness at Equifax at the time of the Data Breach. On information and belief, in this role at Equifax Mr. Payne was responsible for delivery of the IT Business Strategic plan, including IT Risk Governance to manage all risks related to Technology. This includes Access Management, deliverables required for Internal and External auditors, Asset Management, Software compliance, Software license agreement and IT Financial risks.

15. On information and belief, Robert Friedrich, an individual of residence unknown, was the SVP/CIO Global Consumer Solutions at Equifax at the time of the Data Breach. On information and belief, in this role at Equifax Mr. Friedrich was responsible for developing and maintaining Consumer facing platforms and applications for Equifax in the US, UK, and Canada, including platforms for eCommerce and Mobile products.

16. On information and belief, Vidya Sagar Jagadam, an individual of residence unknown, was the Vice President, IT Governance, Risk & Compliance at Equifax at the time of the Data Breach. On information and belief, in this role at Equifax Mr. Jagadam's was responsible for IT Governance, Risk Management, IT Compliance with Security and Regulatory requirements, Identity & Access Management, PCI program, IT Controls and Compliance.

17. On information and belief, Lara Pearson, an individual of residence unknown, was the Senior Director of Risk Security Programs at Equifax at the time of the Data Breach. On information and belief, in this role at Equifax Ms. Pearson was responsible for Information Security Risk and Compliance and leading highly visible information security programs and was experienced in Information Security Policy & Standard Development.

18. On information and belief, Shea Giesler, an individual of residence unknown, was the Vice President, Security Programs at Equifax at the time of the Data Breach. On information and belief, in this role at Equifax Mr. Giesler was responsible for global strategy for ISO 27001 (information security management system standard) compliance, national strategy for FISMA compliance, development of all company security policies, development of security metrics reportable to the CSO, and the security exception process and first level review team.

19. On information and belief, Cliff Barbier, an individual of residence unknown, was the Director, Security Engineering Solutions at Equifax at the time of the Data Breach. On information and belief, in this role at Equifax Mr. Barbier was responsible for information security issues and proper governance, risk management, & compliance.

20. On information and belief, Joe Sanders, an individual of residence unknown, was the Senior Director of Security Engineering Solutions at Equifax at the time of the Data Breach. On information and belief, in this role at Equifax Mr. Sanders was responsible for Application Security and Vulnerability Management Global Leader, Data Loss Prevention, Application Security, and Vulnerability Management, Monitoring and responding to intrusion prevention systems alerts.

21. Plaintiff does not know the true names or capacities, whether individual, associate, corporate, or otherwise, of the defendants sued herein as DOES 1 through 25, inclusive, and Plaintiff therefore sue said defendants by such

fictitious names. Plaintiff will amend this Complaint to state the true names and capacities of these defendants once Plaintiff discovers this information. Plaintiff is informed and believes, and based thereon alleges, that like Mauldin, Hannan, Payne, Boutin, Friedrich, Jagadam, Pearson, Giesler, Barbier, Sanders, each of the DOE Defendants sued herein by a fictitious name is in some way liable and responsible to Plaintiff on the facts herein alleged for Plaintiff's damages in connection with the Data Breach and the negligent operations of Equifax, either as employees or officers of Equifax responsible for ensuring that massive security lapses that led to the Data Breach or negligent reporting that followed its discovery did not occur, or as contractors, subsidiaries, or others to whom Equifax and its officers and employees delegated such authority. Equifax, Smith, Mauldin, Hannan, Payne, Boutin, Friedrich, Jagadam, Pearson, Giesler, Barbier, Sanders, and DOES 1 through 25, inclusive shall be referred to collectively as "Defendants."

III. JURISDICTION AND VENUE.

22. This Court has jurisdiction pursuant to 28 U.S.C. § 1332 because there is complete diversity of citizenship between Plaintiff and Defendants, and the amount in controversy exceeds $75,000, exclusive of interest and costs.

23. This Court has personal jurisdiction over Equifax because Equifax maintains offices in California, conducts business in California, and has sufficient minimum contacts with California to satisfy Due Process standards.

24. On information and belief, the Court has personal jurisdiction over defendants Mauldin and the Doe Defendants as a result of sufficient minimum contacts with California in connection with the Data Breach and the harm caused thereby to Plaintiff Block.

25. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL BACKGROUND.

A. EQUIFAX'S BUSINESS OF STOCKPILING PERSONAL INFORMATION

26. Equifax was founded in Atlanta, Georgia, as Retail Credit Company in 1899. Equifax is one of the three main credit reporting companies in the United States. The Company's business revolves around being a secure storehouse for PII, including financial information, and providing a clear financial profile of consumers that lenders and other businesses can rely on.

27. Equifax organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers.

28. Equifax has seen wide growth as a company based on its use of sensitive financial and personal consumer data. From 2015 to 2016, the company saw operating revenues grow 18% to $3.14 billion. In 2016, Richard F. Smith, the Chairman of the Board and Chief Executive Officer of Equifax received a total compensation package of $14,964,600. Despite the impact of the public disclosure of the data breach, Equifax's current market capitalization of over $14 billion dollars.

29. Equifax has collected and/or stored PII regarding Carson Block, including his Social Security number, birth date, home driver's license information, and credit card information.

B. EQUIFAX'S ABYSMAL HANDLING OF A MASSIVE BREACH OF ITS STOCKPILE OF CONSUMER PERSONAL INFORMATION

30. From about May 2017 through July 2017, Equifax suffered from a self-described "website application vulnerability" which left Block's PII vulnerable to criminals and cyber-attack.

31. On or about July 29, 2017, Equifax discovered that criminals had exploited the "website application vulnerability" in its system and stolen the PII information of over 143 million individuals.

32. Presumably realizing the severe negative this information would have on Equifax's stock price, three of Equifax insiders made substantial sales of Equifax stock within days of the discovery of the massive Data Breach. On Monday, August 1, 2017, Chief Financial Officer John Gamble sold Equifax shares worth $946,374, approximately 13 percent of his Equifax holdings. On the same day, Joseph Loughran, President of U.S. Information Solutions exercised options to dispose of Equifax stock worth $584,099, approximately 9 percent of his Equifax holdings. On August 2, 2017, Rodolfo Ploder, President of Workforce Solutions, sold $250,458 of Equifax stock, almost 4 percent of his holdings.

33. Among them, these three Equifax senior executives sold Equifax shares worth almost $1.8 million in the days following the discovery of the data breach on July 29, 2017, all while Equifax delayed public disclosure of the breach of the millions of innocent victims that their personal information, which had been compromised due to Equifax's negligence.

34. On September 7, 2017, Equifax issued a press release announcing that "[c]riminals exploited a U.S. website application vulnerability to gain access to certain files" in Equifax systems. The breach began in mid-May and continued until it was discovered by Equifax on July 29, 2017. The release stated that "[t]he information accessed primarily include[d] names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal

information for certain UK and Canadian residents." The unauthorized access potentially impacted "approximately 143 million U.S. consumers."

35. Upon this disclosure Equifax shares tumbled over 6 percent from around $142 to around $125 in after-hours trading.

36. Equifax further opted to only notify consumers of the breach via mail if they were among the small percentage whose credit card numbers or dispute documents were accessed. For the remaining millions of consumers, Equifax required them to proactively turn to its poorly designed, unreliable, and potentially insecure website, equifaxsecurity2017.com, where consumers could provide Equifax with personal information to determine whether their data may have been compromised.

37. Equifax also "offered" those impacted by the data breach one year of "complimentary" credit monitoring and identity theft protection, but requiring a consumer's credit card which would be subject to automatic renewal charges if not proactively terminated. Rather than actually attempting to assist the affected consumers, Equifax continued its poor judgment and turned its data breach into a massive marketing opportunity.

C. EQUIFAX'S ONGOING HISTORY OF DATA BREACHES AND LACK OF ADEQUATE PRECAUTIONS.

38. Equifax knew or should have known that its system was at-risk for attack based on previous attacks and reports that its internal system had weaknesses.

39. Equifax knew of problems with its data security, at least as a result of two substantial data breaches that occurred in 2016 alone. In one, hackers took W-2 tax data from an Equifax subsidiary called TALX; the breach (caused by hackers using personal information to guess client customer questions and ultimately reset their 4-digit PIN and gain access to customers' tax data) went undiscovered from nearly a year. In another, Equifax's W-2 Express website was breached in May 2016 (a result of using alarmingly poor security for the generation of PINs from the

last four digits of a SSN and the four digit year of birth) , leading to the leak of 430,000 names, addresses, social security numbers, and other information.

40. Equifax also suffered a smaller data breaches. One in January 2017 concerning LifeLock customer credit information. Another breach of credit reports in 2013-2014 using personal information. In 2016, a vulnerability to cross-site scripting was discovered on Equifax's website, potentially as a result of Equifax using old and discontinued technology. .

41. On September 13, 2017, Equifax confirmed that the Data Breach included the exploit of a US website application vulnerability, Apache Struts CVE-2017-5638. This flaw in Apache Struts framework and the fix for it was publicly disclosed on March 6, 2017. Within days, massive attacks based on the vulnerability were already being reported. More than two months later, the Equifax Data Breach occurred, apparently because Equifax failed to apply the publicly available fix to Apache Struts within its US website applications, despite demonstrable proof and public reporting that the vulnerability gave real-world attackers an easy way to take control of sensitive websites.

FIRST CAUSE OF ACTION

(Negligence- Against All Defendants)

42. Plaintiff re-alleges and incorporates by reference all prior allegations as if fully set forth herein.

43. Defendants owed a duty to Plaintiff to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their personal and financial information in its possession from being compromised, lost stolen, accessed, and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Equifax's security system to ensure that Plaintiffs' and the Class's personal and financial information in Equifax's possession was adequately secured and protected. Defendants further owed a duty to ensure that Equifax's internet security measures were up to date and regularly

tested. Defendants further owed a duty to Plaintiff to implement processes that would detect a breach of it security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

44. Defendants owed a duty to Plaintiffs and the Class to ensure Equifax's security was consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the personal and financial information of Plaintiff held by Equifax.

45. Defendants knew Equifax solicited, gathered, and stored the personal and financial data of Plaintiffs and the Class to facilitate credit reports and monitoring. Defendants knew Equifax inadequately safeguarded such information on its computer systems and that hackers routinely attempt to access this valuable data without authorization. Defendants had prior notice that Equifax's systems were inadequate by virtue of the earlier breaches that preceded this one and by security updates and bulletins regarding systems used by Equifax, but continued to maintain those inadequate systems to the ultimate detriment of consumers like Plaintiff. Defendants knew or should have known that a breach of Equifax systems would cause damages to Plaintiff and Defendants had a duty to adequately protect such sensitive personal and financial information

46. Plaintiff was a foreseeable victims of any inadequate safety and security practices. Plaintiff had no ability to protect the data that was in Equifax's possession from Defendants' negligent security practices, actions, and choices.

47. In addition, Defendants had a duty to timely and adequately disclose to Plaintiff that his PII had been compromised. Such timely disclosure was necessary to allow Plaintiff to take appropriate measures to avoid unauthorized charges to credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor account information and credit reports for fraudulent activity, contact banks or other financial institutions that issue his credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or

ameliorate the damages caused by Defendants' misconduct.

48. Defendants knew, or should have known, the risks inherent in Equifax collecting and storing the personal and financial information of consumers like Plaintiff, and of the critical importance of providing adequate security of that information.

49. Defendants breached their duty to Plaintiff by failing to maintain proper security measures, policies and procedures, and training. Defendants failed to timely notify Plaintiff of the Data Breach, waiting over a month from discovery of the hack to publicly announcing the breach while Equifax executives unloaded stock. Plaintiff has been harmed as a direct and proximate result of Defendants' negligence. Plaintiff will continue to be harmed as a direct and proximate result of Defendants' negligence, including but not necessarily limited to: a) out-of-pocket costs associated with addressing false tax returns filed with the IRS and state tax agencies; b) increased future out of pocket costs in connection with preparing and filing tax returns; c) out-of-pocket costs associated with procuring identity protection and restoration services; d) in the event of future identity theft, out-of-pocket costs associated with repairing credit, reversing fraudulent charges, and other harms; and e) lost productivity and enjoyment as a result of time spent monitoring, addressing and correcting future consequences of the Data Breach.

50. Holding Defendants accountable for their negligence will further the policies underlying negligence law and will require Defendants and encourage similar persons that work with, obtain and retain sensitive consumer personal and financial information to adopt, maintain and properly implement reasonable, adequate and industry-standard security measures to protect such customer information.

51. Plaintiff is entitled to money damages for all out-of-pocket costs caused by Defendants' negligence, and has suffered damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION

(Violation of Unfair Competition Law California Business and Professional Code Section 17200, *et seq.*- Against Equifax)

52. Plaintiff re-alleges and incorporates by reference all prior allegations as if fully set forth herein.

53. Equifax engaged in unfair and unlawful business practices in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, et seq. ("UCL"). Equifax's acts, omissions, and conduct constitute unfair and unlawful business practices under the UCL.

54. Equifax's practices were unlawful and in violation of Civil Code section 1798.81.5 of the Customer Records Act ("CRA") because Equifax failed to take reasonable measures in protecting Plaintiff's PII.

55. Equifax's practices were unlawful and in violation of Civil Code section 1798.82 of the CRA because Equifax failed to timely or adequately disclose that Plaintiff's PII had been breached by hackers.

56. Equifax's acts, omissions, and conduct also constitute "unfair" business acts or practices because they offend public policy and constitute immoral, unethical, and unscrupulous activities that caused substantial injury, to Plaintiff and others. The gravity of harm resulting from Equifax's conduct outweighs any potential benefits attributable to the conduct and there were reasonably available alternatives to further Equifax's legitimate business interests.

57. Equifax has exclusive knowledge about the extent of the Data Breach, including during the days and weeks following the Data Breach.

58. As a direct and proximate result of Equifax's unlawful and unfair business practices as alleged herein, Plaintiff has suffered injury in fact. Plaintiff has been injured in that his personal and financial PII has been compromised, subject to identity theft, identity fraud, and/or is at risk for future identity theft and fraudulent

activity on their financial accounts.

59. As a direct and proximate result of Equifax's unlawful and unfair business practices as alleged herein, Plaintiff already suffers from identity theft, identity and financial fraud, and/or a continuing increased risk of identity theft and financial fraud due to the compromise, publication, and/or unauthorized use of his financial PII. Plaintiff has also been injured by, among other things: (1) the loss of the opportunity to control how his PII is used; (2) the compromise, publication, and/or theft of their PII; (3) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial accounts; (4) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity fraud; (5) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (6) unauthorized use of compromised PII to open new financial accounts; (7) tax fraud and/or other unauthorized charges to financial accounts and associated lack of access to funds while proper information is confirmed and corrected; (8) the continued risk to his PII and the PII of family members which remain in Equifax's possession and are subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect the PII in its possession; and (9) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the Plaintiff's life.

60. As a result of Equifax's violations of the UCL, Plaintiff is entitled to injunctive relief, including, but not limited to an order preventing Equifax from engaging in the negligent practices that lead to the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment against Defendants as follows:

A. A finding that Defendant breached their duty to safeguard and protect Plaintiff's PII which was compromised in the Data Breach;

B. An award of damages against Defendants and in favor of Plaintiff, including actual damages, punitive damages, and/or statutory damages according to proof, but at least $500,000;

C. Award equitable, injunctive, and declaratory relief as appropriate;

D. For attorney fees, costs of suit and prejudgment and post-judgment interest, as provided under applicable law; and

E. For such other, further, and/or different relief, in law or equity, as the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff hereby demands a trial by jury, including pursuant to Federal Rule of Civil Procedure 38(b), on all issues where a right to such trial exists.

Dated: September 15, 2017

RAINES FELDMAN LLP

By: */s/ Erik S. Syverson*
ERIK S. SYVERSON
Attorneys for Plaintiff Carson Block

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of California

CARSON BLOCK, an individual

Plaintiff(s)

v.

EQUIFAX, INC., a Georgia Corporation; RICHARD F. SMITH, an Individual, SUSAN MAULDIN, an Individual, MARY HANNAN, an Individual, GRAEME PAYNE, an Individual, HAROLD BOUTIN, an Individual, ROBERT FRIEDRICH, an Individual, VIDYA SAGAR JAGADAM, an Individual, LARA PEARSON, an Individual, SHEA GIESLER, an Individual, CLIFF BARBIER, an Individual, JOE SANDERS, an Individual, and DOES 1 through 25, inclusive

Defendant(s)

Civil Action No. 17-5367

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Erik S. Syverson (Bar No. 221933)
RAINES FELDMAN LLP
1800 Avenue of the Stars, 12th Floor, Los Angeles, California 90067
Telephone: (310) 440-4100, Facsimile: (310) 765-7730
esyverson@raineslaw.com

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____

☐ I personally served the summons on the individual at *(place)* _____ _____ on *(date)* _____; or

☐ I left the summons at the individual's residence or usual place of abode with *(name)* _____ _____, a person of suitable age and discretion who resides there, on *(date)* _____, and mailed a copy to the individual's last known address; or

☐ I served the summons on *(name of individual)* _____, who is designated by law to accept service of process on behalf of *(name of organization)* _____ _____ on *(date)* _____; or

☐ I returned the summons unexecuted because _____; or

☐ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ _____

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

JS-CAND 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS-CAND 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 in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

CARSON BLOCK, an individual

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Erik S. Syverson (Bar No. 221933)
RAINES FELDMAN LLP
1800 Avenue of the Stars, 12th Fl., LA, CA 90067
Telephone: (310) 440-4100, Facsimile: (310) 765-7730

DEFENDANTS

EQUIFAX, INC., a Georgia Corporation; RICHARD F. SMITH, an Individual, SUSAN MAULDIN, an Individual, MARY HANNAN, an Individual, GRAEME PAYNE, an Individual, HAROLD BOUTIN, an Individual, ROBERT FRIEDRICH, an Individual, VIDYA SAGAR JAGADAM, an Individual, LARA PEARSON, an Individual, SHEA GIESLER, an Individual, CLIFF BARBIER, an Individual, JOE SANDERS, an Individual, and DOES 1 through 25, inclusive

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)*

CONTRACT

- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 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 & 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)***:

Brief description of cause:

(1) Negligence; and; (2) Violations of Unfair Competition Law (Cal. Bus. & Prof. Code § 17200, et seq.

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

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE September 15, 2017 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Erik S. Syverson

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 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 in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate 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 Federal Rule of Civil Procedure 8(a), 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.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 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.

(4) Diversity of citizenship. This refers to suits under 28 USC § 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-CAND 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 the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

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 Federal Rule of Civil Procedure 23.

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-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

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