Daniel S. Robinson, CA Bar No. 244245
drobinson@robinsonfirm.com
Scot D. Wilson, CA Bar No. 223367
swilson@robinsonfirm.com
Wesley K. Polischuk, CA Bar No. 254121
wpolischuk@robinsonfirm.com
ROBINSON CALCAGNIE, INC.
19 Corporate Plaza Dr.
Newport Beach, CA 92660
Telephone: (949) 720-1288
Fax: (949) 720-1292

Counsel for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

GRANT AVISE, individually and on behalf of all others similarly situated,

Plaintiff,

v.

EQUIFAX, INC.,

Defendant.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff GRANT AVISE, individually and on behalf of the classes defined below, bring this Class Action Complaint ("Complaint") against Equifax, Inc. ("Equifax"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, and allege as follows:

NATURE OF THE CASE

1. On September 7, 2017, Equifax announced a nationwide data breach affecting an estimated 143 million consumers (the "Data Breach"). According to Equifax's press release and other public statements, unauthorized parties accessed consumers' sensitive, personal information maintained by Equifax by exploiting a website application vulnerability. Equifax claims that based on its investigation, the unauthorized access occurred from mid-May through July 2017. The information included names, addresses, Social Security numbers, dates of birth, and, in some instances, driver's license numbers. Equifax as also admitted that credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information ("PII") for approximately 182,000 U.S. consumers.[1]

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

3. Armed with the personal information obtained in the Data Breach, identity thieves can commit a variety of crimes that harm victims of the Data Breach. For instance, they can take out loans, mortgage property, and open financial accounts and

[1] *See Cybersecurity Incident & Important Consumer Information*, EQUIFAX, https://www.equifaxsecurity2017.com/ (last visited Sept. 8, 2017).

credit cards in a victim's name; use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in a victim's name; obtain medical services in a victim's name; or give false information to police during an arrest. Hackers also routinely sell individuals' PII to other criminals who intend to misuse the information.

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

5. There is a strong likelihood that Class members already have or will become victims of identity fraud given the breadth of their PII that is now publicly available. Javelin Strategy & Research reported in its 2014 Identity Fraud Study that "[d]ata breaches are the greatest risk factor for identity fraud." In fact, "[i]n 2013, one in three consumers who received notification of a data breach became a victim of fraud." Javelin also found increased instances of fraud other than credit card fraud, including "compromised lines of credit, internet accounts (e.g., eBay, Amazon) and email payment accounts such as PayPal."

6. Plaintiff brings this action to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff seeks the following remedies, among others: statutory damages under the Fair Credit Reporting Act ("FCRA") and state consumer protection statutes, reimbursement

of out-of-pocket losses, other compensatory damages, further 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.

PARTIES

7. Plaintiff GRANT AVISE is a resident of Orange, California and was a California resident during the period of the Data Breach. Plaintiff GRANT AVISE previously provided his PII to Equifax, including but not limited to his name, Social Security number and date of birth. Plaintiff GRANT AVISE is a victim of the Data Breach. As a result of the Data Breach, Plaintiff GRANT AVISE paid out-of-pocket for services to protect his identity. Plaintiff GRANT AVISE has also spent time and effort monitoring his financial accounts, and anticipates spending more time and effort in the future as a result of the Data Breach.

8. Defendant Equifax, Inc. is a Delaware corporation with its principal place of business located at 1550 Peachtree Street NE Atlanta, Georgia 30309. Equifax, Inc. may be served through its registered agent, Shawn Baldwin, at its principal office address identified above.

9. Equifax is one of the major credit reporting bureaus in the United States. As a credit bureau service, Equifax is engaged in a number of credit-related services for individuals, businesses, and compliance with government regulations. Specifically, Equifax provides business services to the automotive, communications, utilities and digital media, education, financial services, healthcare, insurance, mortgage, restaurant, retail and wholesale trade, staffing, and transportation and distribution industries.[2] Equifax markets and sells many products to consumers and businesses, including Consumer Reports, which provides "access to current personally identifiable

[2] *See Equifax's Business Industries*, EQUIFAX, http://www.equifax.com/business/ (last visited Sept. 8, 2017).

information for over 210 million consumers."[3] Equifax's Consumer Reports also includes "tradelines on over 1.8 billion trades updated monthly" and "600 million unique, annual inquiries." Equifax's Consumer Reports provides "access to the consumer's name, current address, address, previous former addresses, birth date, former names and Social Security number." Equifax's Consumer Reports is a product designed to "increase revenue"[4]:

> **Make effective decisions that increase revenue**
>
> Trust Equifax Consumer Reports to deliver the powerful combination of predictive consumer credit data and proven expertise backed by unmatched industry leadership. Make faster decisions with the competitive advantage of data speed and system integrity. Strengthen predictive ability, mitigate risk, manage acquisition costs and increase revenue with proven decisioning insight from Equifax Consumer Reports.

JURISDICTION AND VENUE

10. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because Plaintiffs are bringing claims under the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681e, *et seq*.

11. This Court also 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.

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

FACTS

A. The Data Breach Compromised the PII of 143 Million Consumers

13. On September 7, 2017, Equifax announced that its systems had been breached and that the Data Breach affected approximately 143 million consumers.

---

[3] *See Equifax's Consumer Reports Product Overview*, EQUIFAX, http://www.equifax.com/business/consumer-reports (last visited Sept. 8, 2017).

[4] *See Equifax's Consumer Reports Product Sheet*, EQUIFAX, http://www.equifax.com/assets/USCIS/efx-00198_consumer_reports.pdf (last visited Sept. 8, 2017).

According to Equifax's website regarding the Data Breach, unauthorized users acquired the PII of approximately 143 million consumers from certain files maintained and stored by Equifax. The PII included names, addresses, Social Security numbers, dates of birth, and, in some instances, driver's license numbers, and other personal information:

> Equifax today announced a cybersecurity incident potentially impacting approximately ***143 million U.S. consumers***. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017.
>
> …
>
> The information accessed primarily includes ***names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers***. In addition, ***credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers***, were accessed.[5]

14. On its website, Equifax admits learning of the Data Breach on July 29, 2017, but only began notifying consumers through a press release and generic website at https://www.equifaxsecurity2017.com on September 7, 2017, almost 4 months after the Data Breach began.[6]

15. Instead of immediately notifying consumers when it discovered the Data Breach, Equifax executives sold at least $1.8 million worth of shares before the public disclosure of the breach. It has been reported that its Chief Financial Officer John Gamble sold shares worth $946,374, its president of U.S. information solutions, Joseph

[5] *See Cybersecurity Incident & Important Consumer Information*, EQUIFAX, https://www.equifaxsecurity2017.com/ (last visited Sept. 8, 2017).

[6] *See Cybersecurity Incident & Important Consumer Information*, EQUIFAX, https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last visited Sept. 8, 2017).

Loughran, exercised options to dispose of stock worth $584,099, and its president of workforce solutions, Rodolfo Ploder, sold $250,458 of stock on August 2, 2017.[7]

16. In response to the questions of "Why am I learning about this incident through the media?" and "Why didn't Equifax notify me directly?", Equifax states that it "issued a national press release in order to notify U.S. consumers of this incident and has established a website, www.equifaxsecurity2017.com, where U.S. consumers can receive further information."[8]

17. Despite the fact that Equifax has the names and addresses for the 143 million U.S. Data Breach victims, Equifax has not provided direct mail notices to them; rather, Equifax states that it will only provide direct mail notice to the 209,000 consumers whose credit card numbers and 182,000 U.S. consumers whose dispute documents with PII were impacted.[9]

18. On its website, Equifax admits the unauthorized disclosure of consumer data and warned consumers of the consequences of the Data Breach:

> We recommend that consumers be vigilant in reviewing their account statements and credit reports, and that they immediately report any unauthorized activity to their financial institutions. We also recommend that they monitor their personal information and visit the Federal Trade Commission's, website, www.ftc.gov/idtheft, to obtain information about steps they can take to better protect against identity theft as well as information about fraud alerts and security freezes.[10]

---

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

[8] *Id.*

[9] *See Cybersecurity Incident & Important Consumer Information*, EQUIFAX, https://www.equifaxsecurity2017.com/ (last visited Sept. 8, 2017).

[10] *See Cybersecurity Incident & Important Consumer Information*, EQUIFAX, https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last visited Sept. 8, 2017).

19. On its Data Breach website, Equifax invites individuals to determine if their personal information may have been impacted by the Data Breach by providing their last name and the last 6 digits of their Social Security number. If an individual is determined to have been affected, Equifax provides them with a date to return to the website to enroll in Equifax's TrustedID Premier credit monitoring service. If an individual is determined to have not been affected, Equifax provides them with this information, but then still provides them with a link to enroll in (and pay for) Equifax's TrustedID Premier credit monitoring service.

B. Equifax Promised to Protect Its Customers' PII, but Maintained Inadequate Data Security

20. Equifax is one of the major credit reporting bureaus in the United States. As a credit bureau service, Equifax is engaged in a number of credit-related services for individuals, businesses, and compliance with government regulations. Specifically, Equifax provides business services to the automotive, communications, utilities and digital media, education, financial services, healthcare, insurance, mortgage, restaurant, retail and wholesale trade, staffing, and transportation and distribution industries.[11] Equifax markets and sells many products to consumers and businesses, including Consumer Reports, which provides "access to current personally identifiable information for over 210 million consumers."[12] Equifax's Consumer Reports also includes "tradelines on over 1.8 billion trades updated monthly" and "600 million unique, annual inquiries." Equifax's Consumer Reports provides "access to the consumer's name, current address, address, previous former addresses, birth date, former names and Social Security number."[13]

21. Prior to the Data Breach, Equifax promised its customers and everyone else

[11] *See Equifax's Business Industries*, EQUIFAX, http://www.equifax.com/business/ (last visited Sept. 8, 2017).

[12] *See Equifax's Consumer Reports Product Overview*, EQUIFAX, http://www.equifax.com/business/consumer-reports (last visited Sept. 8, 2017).

[13] *See Equifax's Consumer Reports Product Sheet*, EQUIFAX, http://www.equifax.com/assets/USCIS/efx-00198_consumer_reports.pdf (last visited Sept. 8, 2017).

whose PII it collects that it would reasonably protect their PII. Equifax's privacy policy stated, in relevant part:

> We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to ***protect the privacy and confidentiality of personal information about consumers***. We also protect the sensitive information we have about businesses. ***Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.***[14]

22. Equifax's policy further stated:

> We are committed to protecting the security of your information through procedures and technology designed for this purpose by taking these steps:
>
> - We limit access to your personal information to employees having a reasonable need to access this information to provide products and services to you. Employees who misuse information are subject to disciplinary action, including termination.
>
> - We have reasonable physical, technical and procedural safeguards to help protect your personal information.
>
> - In areas that contain your personal information, we use secure socket layer (SSL) encryption to help protect this information while it is in transit between our servers and your computer.[15]

23. Plaintiff and Class members disclosed their PII to Equifax in connection with consumer transactions and Equifax compiled, maintained, furnished, and made

[14] *See Equifax's Privacy Policy*, EQUIFAX, http://www.equifax.com/privacy/ (last visited Sept. 8, 2017).

[15] *See Equifax's Personal Credit Reports Privacy Policy*, EQUIFAX, http://www.equifax.com/privacy/ (last visited Sept. 8, 2017).

available Plaintiff's and Class members' PII. Equifax was allowed to perform such services involving sensitive information only if it adhered to the requirements of laws meant to protect the privacy of such information, such as the FCRA and the Gramm-Leach-Bliley Act ("GLBA"). Equifax's maintenance, use, and furnishing of such PII is and was intended to affect Plaintiff and other Class members, and the harm caused by disclosure of that PII in the Data Breach was entirely foreseeable to Equifax.

C. Equifax Experienced Prior Data Breaches, but Nevertheless Failed to Implement Appropriate Security

24. Although Equifax claims to be a leader in data security and its privacy policy promises to reasonably safeguard consumer data, Equifax's own data security practices were inadequate. Equifax was well aware of this fact because it had experienced multiple data breaches in recent years.

25. In March 2014, Equifax reported a data breach to the New Hampshire Attorney General involving an IP address operator who was able to obtain Equifax consumer credit reports using sufficient personal information to bypass Equifax's identity verification process.[16]

26. In May 2016, Equifax's W-2 Express website suffered a data breach where an attacker was able to access, download and post the names, addresses, social security numbers and other personal information of over 430,000 Kroger employees. The attackers were able to access the W-2 data by merely entering Equifax's portal with an employee's default PIN code, which was the last four digits of the employee's Social Security number and their four-digit birth year.[17]

27. Independent security researchers have also found that Equifax's website is

[16] *See Letter from Troy G. Kubes, Vice President & Associate Group Counsel at Equifax Legal Department, to Attorney General Joseph Foster*, MAR. 5, 2014, https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20140305.pdf (last visited Sept. 8, 2017).

[17] *See Crooks Grab W-2s from Credit Bureau Equifax*, KREBS ON SECURITY, http://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/ (last visited Sept. 8, 2017).

vulnerable. In 2016, a security researcher found a common vulnerability known as cross-site scripting (XSS) on the main Equifax website. Such XSS bugs allow attackers to send specially-crafted links to Equifax customers and, if the target clicks through and is logged into the site, their username and password can be revealed to the hacker.[18]

28. Researcher Kenneth White just recently discovered a link in the source code on the Equifax consumer sign-in page that pointed to Netscape, a web browser that was discontinued in 2008. Kevin Beaumont, a British security professional, found decade-old software in use, including IBM WebSphere, Apache Struts and Java, many of which are outdated and subject to well-known vulnerabilities.[19]

D. The Data Breach Has Exposed Plaintiffs and Other Consumers to Fraud, Identity Theft, Financial Harm, and a Heightened, Imminent Risk of Such Harm in the Future

29. Since identity thieves use the PII of other people to commit fraud or other crimes, Plaintiffs and other consumers whose information was exposed in the Data Breach are subject to an increased, concrete risk of identity theft. Javelin Strategy & Research, a research-based consulting firm that specializes in fraud and security in advising its clients, reported in its 2014 Identity Fraud Study that "[d]ata breaches are the greatest risk factor for identity fraud." In fact, "[i]n 2013, one in three consumers who received notification of a data breach became a victim of fraud." Javelin also found increased instances of fraud other than credit card fraud, including "compromised lines of credit, internet accounts (*e.g.*, eBay, Amazon) and email payment accounts such as PayPal."[20]

30. The exposure of Plaintiff's and Class members' Social Security numbers in particular poses serious problems. Criminals frequently use Social Security numbers to

[18] *See A Brief History Of Equifax Security Fails*, FORBES, https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#53a60715677c (last visited Sept. 8, 2017).

[19] *Id.*

[20] *See* https://www.javelinstrategy.com/press-release/new-identity-fraud-victim-every-two-seconds-2013-according-latest-javelin-strategy (last visited April 14, 2016).

create false bank accounts, file fraudulent tax returns, and incur credit in the victim's name. Neal O'Farrell, a security and identity theft expert for Credit Sesame calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers."[21] Even where data breach victims obtain a new Social Security number, the Social Security Administration warns "that a new number probably will not solve all [] problems . . . and will not guarantee [] a fresh start."[22] In fact, "[f]or some victims of identity theft, a new number actually creates new problems." One of those new problems is that a new Social Security number will have a completely blank credit history, making it difficult to get credit for a few years unless it is linked to the old compromised number.

31. As a result of the compromising of their personal information, Plaintiff and Class members will face an increased risk of experiencing the following injuries:

- money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;
- money and time lost as a result of fraudulent access to and use of their financial accounts;
- loss of use of and access to their financial accounts and/or credit;
- impairment of their credit scores, ability to borrow, and/or ability to obtain credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs and lost time obtaining credit reports in order to monitor their credit records;
- money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;

[21] Tips, How to Protect Your Kids From the Anthem Data Breach," Kiplinger (Feb. 10, 2015), *available at* http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html (last visited April 14, 2016).

[22] Social Security Administration, Identity Theft and Your Social Security Number, pp. 7-8, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 10, 2016)

- money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
- costs of credit monitoring that is more robust than the services being offered by Equifax;
- anticipated future costs from the purchase of credit monitoring and/or identity theft protection services once the temporary services being offered by Equifax expire;
- costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;
- money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;
- lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach, including but not limited to efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;
- loss of the opportunity to control how their personal information is used; and
- continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Equifax fails to undertake appropriate, legally required steps to protect the personal information in its possession.

32. The risks that Plaintiff and Class members bear as a result of the Data Breach cannot be mitigated by the credit monitoring Equifax has offered to affected consumers because it can only help detect, but will not prevent, the fraudulent use of Plaintiff's and Class members' PII. Instead, Plaintiff and Class members will need to

spend time and money to protect themselves. For instance, credit reporting agencies impose fees for credit freezes in certain states. In addition, while credit reporting agencies offer consumers one free credit report per year, consumers who request more than one credit report per year from the same credit reporting agency (such as Equifax) must pay a fee for the additional report. Such fees constitute out-of-pocket costs to Plaintiff and Class members.

33. The risks borne by affected consumers are not hypothetical: Equifax has admitted that Class members' personal information was disclosed and downloaded in the Data Breach, has admitted the risks of identity theft, and has encouraged consumers to vigilantly monitor their accounts.

D. Equifax Was Required to Investigate and Provide Timely and Adequate Notification of the Data Breach under Federal Regulations

34. 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. 15 U.S.C. § 6801(b) (emphasis added).

35. In order 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.

36. 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.* "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).

37. 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.*

38. Credit bureaus are "financial institutions" for purposes of the GLBA, and are therefore subject to its provisions. *See TranUnion LLC v. F.T.C.*, 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[23]" are "so closely related to banking or managing or controlling banks as to be a proper incident thereto." Since Equifax is a credit bureau and performs credit bureau services, it qualifies as a financial institution for purposes of the GLBA.

39. "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.

40. 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." This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Class members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that its data security

[23] 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." *See* 12 C.F.R. § 225.28.

practices were inadequate to safeguard Class members' PII.

41. 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" as mandated by the GLBA. 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.

42. Upon information and belief, Equifax also failed to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information.

CLASS ACTION ALLEGATIONS

43. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4).

A. Nationwide Class

44. Plaintiff bring his FCRA, negligence, and negligence per se claims (Counts I-IV) on behalf of a proposed nationwide class ("Nationwide Class"), defined as follows:

> *All natural persons and entities in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Equifax in September 2017.*

B. Statewide Classes

45. Plaintiff bring his state consumer protection statute and data breach notification claims (Counts V through VII) on behalf of a separate California Subclass.

46. Plaintiff also brings his negligence and negligence per se claims (counts III and IV) separately on behalf of the California Subclass, in the alternative to bringing those claims on behalf of the Nationwide Class.

47. Except where otherwise noted, "Class members" shall refer to members of the Nationwide Class and California Subclass, collectively.

48. Excluded from the Nationwide Class and California Subclass are Defendants and their current employees, as well as the Court and its personnel presiding over this action.

49. The Nationwide and California Subclass meet the requirements of Federal Rules of Civil Procedure 23(a) and 23(b)(1), (b)(2), and (b)(3) for all of the reasons set forth in Paragraphs 39-47:

50. **Numerosity:** The Nationwide and California Subclass are so numerous that joinder of all members is impracticable. According to Equifax, the Nationwide Class includes approximately 143 million individuals whose PII was acquired during the Data Breach. On information and belief, Plaintiff alleges that there are millions of individuals in the California Subclass. The parties will be able to identify each member of the Nationwide Class and California Subclass after Equifax's document production and/or related discovery.

51. **Commonality:** There are numerous questions of law and fact common to Plaintiff and the Nationwide and California Subclass, including but not limited to the following:

- whether Equifax engaged in the wrongful conduct alleged herein;
- whether Equifax owed a duty to Plaintiff and Class members to adequately protect their PII;
- whether Equifax breached its duties to protect the personal information of Plaintiff and Class members;
- whether Equifax knew or should have known that its data security systems and processes were vulnerable to attack;
- whether Plaintiff and Class members suffered legally cognizable damages as a result of Equifax's conduct, including increased risk of identity theft and loss of value of PII;

- whether Equifax violated the FCRA; and
- whether Plaintiff and Class members are entitled to equitable relief including injunctive relief.

52. **Typicality:** Plaintiff's claims are typical of the claims of the Nationwide Class, and Plaintiff's claims are typical of the claims of the California Subclass. Plaintiff, like all proposed Class members, had his PII compromised in the Data Breach.

53. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Nationwide Class and California Subclass. Plaintiff has no interests that are adverse to, or in conflict with, the Class members. There are no claims or defenses that are unique to Plaintiff. Likewise, Plaintiff has retained counsel experienced in class action and complex litigation, including data breach litigation, that have sufficient resources to prosecute this action vigorously.

54. **Predominance:** The proposed action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Nationwide Class and California Subclass predominate over any questions which may affect only individual Class members in any of the proposed classes.

55. **Superiority:** 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.

56. 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.

57. **Risks of Prosecuting Separate Actions:** Plaintiff's claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of

separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Equifax. Equifax continues to maintain the PII of the Class members and other individuals, and varying adjudications could establish incompatible standards with respect to: Equifax's duty to protect individuals' PII; whether Equifax's ongoing conduct violates the FCRA and other claims alleged herein; and whether the injuries suffered by Class members are legally cognizable, among others. Prosecution of separate actions by individual Class members would also create a risk of individual adjudications that would be dispositive of the interests of other Class members not parties to the individual adjudications, or substantially impair or impede the ability of Class members to protect their interests.

58. **Injunctive Relief:** In addition, Equifax has acted and/or refused to act on grounds that apply generally to the Nationwide and California Subclass, making injunctive and/or declaratory relief appropriate with respect to the classes under Federal Rule of Civil Procedure 23(b)(2). Equifax continues to (1) maintain the PII of Class members, (2) fail to adequately protect their PII, and (3) violate their rights under the FCRA and other claims alleged herein.

59. **Certification of Particular Issues:** In the alternative, the Nationwide and California Subclass may be maintained as class actions with respect to particular issues, in accordance with Fed. R. Civ. P. 23(c)(4).

CAUSES OF ACTION

COUNT I

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

(On Behalf of the Nationwide Class)

60. Plaintiff incorporates by reference all paragraphs above as if fully set forth herein.

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

62. Under the FCRA, a "consumer reporting agency" is defined as "any person

which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

63. Equifax is a consumer reporting agency under the FCRA because for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

64. As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

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

66. The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

67. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown

entities, or computer hackers such as those who accessed the Nationwide Class members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

68. Equifax furnished the Nationwide Class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

69. The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.[24]

70. Equifax willfully violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. The willful nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

71. Equifax also acted willfully because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the

[24] Statement of Commissioner Brill (Federal Trade Commission 2011), *available at* <https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonestatement.pdf> (last visited Apri 14, 2016).

promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiff and other members of the classes of their rights under the FCRA.

72. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiff's and Nationwide Class members' personal information for no permissible purposes under the FCRA.

73. Plaintiff and the Nationwide Class members have been damaged by Equifax's willful failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A) (emphasis added).

74. Plaintiffs and the Nationwide Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2), (3).

COUNT II

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

(On Behalf of the Nationwide Class)

75. Plaintiff incorporates by reference all paragraphs above as if fully set forth here.

76. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that

Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

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

78. Plaintiff and the Nationwide Class members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiff and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

79. Plaintiff and the Nationwide Class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT III

NEGLIGENCE

(On Behalf of the Nationwide Class and California Subclass)

80. Plaintiff incorporates by reference all paragraphs above as if fully set forth here.

81. Equifax owed a duty to Plaintiff and Class members, arising from the sensitivity of the information and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class members' information adequately secured from unauthorized access.

82. Equifax's privacy policy acknowledged Equifax's duty to adequately protect Class members' PII.

83. Equifax owed a duty to Class members to implement current and available technology that would prevent foreseeable data breaches, such as this one.

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

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

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

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

88. Equifax had a special relationship with Plaintiff and Class members from being entrusted with their PII, which provided an independent duty of care. Plaintiff's and other Class members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, Equifax had the ability to protect its systems and the PII it stored on them from attack.

89. Equifax's role to utilize and purportedly safeguard Plaintiff's and Class members' PII presents unique circumstances requiring a reallocation of risk.

90. 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 Equifax's data security practices were inadequate to safeguard Class members' PII; and (d) failing to provided adequate and timely notice of the Data Breach.

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

92. Plaintiff 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.

93. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiff's and the Nationwide Class members' PII and consumer reports for no

permissible purposes under the FCRA.

94. As a result of Equifax's willful failure to prevent the Data Breach, Plaintiff 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. Plaintiff and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class members' PII has also diminished the value of the PII.

95. The damages to Plaintiff and the Class members were a proximate, reasonably foreseeable result of Equifax's breaches of its duties.

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

COUNT IV

NEGLIGENCE PER SE

(On behalf of the Nationwide Class and California Subclass)

97. Plaintiff incorporates by reference all paragraphs above as if fully set forth here.

98. Under the FCRA, 15 U.S.C. §§ 1681e, Equifax is required to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

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

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

101. As alleged above, Equifax was required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards:

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

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

103. 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.*

104. 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.*

105. Equifax violated by GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This

includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Class members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Equifax's data security practices were inadequate to safeguard Class members' PII.

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

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

108. Plaintiff 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.

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

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

111. As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiff 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. Plaintiff and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other

protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff and Class members' PII has also diminished the value of the PII.

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

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

COUNT V

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code § 17200, *et seq*.

(On Behalf of the Nationwide Class or, in the Alternative, the California Subclass)

114. Plaintiff incorporates by reference all paragraphs above as if fully set forth herein.

115. California Business & Professions Code § 17200 prohibits any "unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." For the reasons discussed above, Equifax violated (and continues to violate) California's Unfair Competition Law, California Business & Professions Code § 17200 *et seq.*, by engaging in the above-described unlawful, unfair, fraudulent, deceptive, untrue, and misleading acts and practices.

116. Equifax's unfair and fraudulent acts and practices include but are not limited to the following:

a. Equifax failed to enact adequate privacy and security measures, in California, to protect the Class members' PII from unauthorized disclosure, release, data breaches, and theft, in violation of industry standards and best practices, which was a direct and proximate cause of the Data Breach;

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

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

d. Equifax knowingly and fraudulently misrepresented that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class members' PII;

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

f. Equifax failed to maintain reasonable security, in violation of Cal. Civ. Code § 1798.81.5; and

g. Equifax failed to disclose the Data Breach to Class members in a timely and accurate manner, in violation of the duties imposed by Cal. Civ. Code § 1798.82 *et seq*.

117. Equifax's acts and practices also constitute "unfair" business acts and practices, in that the harm caused by Equifax's wrongful conduct outweighs any utility of such conduct, and such conduct (i) offends public policy, (ii) is immoral, unscrupulous, unethical, oppressive, deceitful and offensive, and/or (iii) has caused and will continue to cause substantial injury to consumers such as Plaintiff and Class members.

118. Equifax's acts and practices also constitute "unlawful" business acts and practices by virtue of their violation of the FCRA, 15 U.S.C. §§ 1681e (as described fully above), the GLBA, 15 U.S.C. § 6801 *et seq.* (as described fully above), California's fraud and deceit statutes, Cal. Civ. Code §§ 1572, 1573, 1709, 1711; Cal. Bus. & Prof. Code §§ 17200, *et seq*., 17500, *et seq*., the California Customer Records' Act, Cal. Civ. Code §§ 1798.80, *et seq*. (as described fully below), and California common law.

119. There were reasonably available alternatives to further Equifax's legitimate

business interests, including using best practices to protect Class members' PII, other than Equifax's wrongful conduct described herein.

120. As a direct and/or proximate result of Equifax's unfair practices, Plaintiff, the Nationwide Class, and the California Subclass have suffered injury in fact in connection with the Data Breach, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII. As a result, Plaintiff and other Class members are entitled to compensation, restitution, disgorgement, and/or other equitable relief. Cal. Bus. & Prof. Code § 17203.

121. Equifax knew or should have known that its data security practices and infrastructure were inadequate to safeguard Class members' PII, and that the risk of a data breach or theft was highly likely. Equifax's actions in engaging in the above named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to Class members' rights.

122. On information and belief, Equifax's unlawful and unfair business practices, except as otherwise indicated herein, continue to this day and are ongoing.

123. Plaintiff and other Class members also are entitled to injunctive relief, under California Business and Professions Code §§ 17203, 17204, to stop Equifax's wrongful acts and to require Equifax to maintain adequate security measures to protect the personal and financial information in its possession.

124. Under Business and Professions Code § 17200 *et seq.*, Plaintiff seeks restitution of money or property that Equifax may have acquired by means of Equifax's deceptive, unlawful, and unfair business practices (to be proven at trial), restitutionary disgorgement of all profits accruing to Equifax because of its unlawful and unfair business practices (to be proven at trial), declaratory relief, and attorney's fees and costs (allowed by Cal. Code Civil Pro. §1021.5).

/ / /

COUNT VI

VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT

Cal. Civ. Code § 1798.80, *et seq.*

(On Behalf of the California Subclass)

125. Plaintiff incorporates by reference all paragraphs above as if fully set forth herein.

126. "[T]o ensure that personal information about California residents is protected," Civil Code § 1798.81.5 requires any "business that owns, licenses, or maintains personal information about a California resident [to] implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

127. Equifax owns, maintains, and licenses personal information, within the meaning of § 1798.81.5, about Plaintiff and the California Subclass.

128. Equifax violated Civil Code § 1798.81.5 by failing to implement reasonable measures to protect Class members' PII.

129. As a direct and proximate result of Equifax's violations of section 1798.81.5 of the California Civil Code, the Data Breach described above occurred.

130. In addition, California Civil Code § 1798.82(a) provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay . . . ."

131. Section 1798.2(b) provides that "[a] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the

security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

132. Equifax is a business that own or license computerized data that include personal information as defined by Cal. Civ. Code § 1798.80 *et seq*.

133. In the alternative, Equifax maintains computerized data that includes personal information that Equifax does not own as defined by Cal. Civ. Code § 1798.80 *et seq*.

134. Plaintiff and the California Subclass members' PII (including but not limited to names, addresses, and Social Security numbers) includes personal information covered by Cal. Civ. Code § 1798.81.5(d)(1).

135. Because Equifax reasonably believed that Plaintiff and the California Subclass members' personal information was acquired by unauthorized persons during the Data Breach, it had an obligation to disclose the Data Breach in a timely and accurate fashion under Cal. Civ. Code § 1798.82(a), or in the alternative, under Cal. Civ. Code § 1798.82(b).

136. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated Cal. Civ. Code § 1798.82.

137. As a direct and proximate result of Equifax's violations of sections 1798.81.5 and 1798.82 of the California Civil Code, Plaintiff and the California Subclass Members suffered the damages described above, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

138. Plaintiff and the California Subclass seek relief under § 1798.84 of the California Civil Code, including, but not limited to, actual damages in an amount to be proven at trial, and injunctive relief.

/ / /

/ / /

COUNT VII

VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT

Cal. Civ. Code § 1750, et seq.

(On Behalf of the California Subclass)

139. Plaintiff incorporates by reference all paragraphs above as if fully set forth herein.

140. The Consumers Legal Remedies Act, California Civil Code § 1750, *et seq.* (the "CLRA") has adopted a comprehensive statutory scheme prohibiting various deceptive practices in connection with the conduct of a business providing goods, property, or services to consumers primarily for personal, family, or household purposes. The self-declared purposes of the CLRA are to protect consumers against unfair and deceptive business practices and to provide efficient and economical procedures to secure such protection.

141. Equifax is a "person" as defined by Civil Code Section 1761(c), because Equifax is a corporation as set forth above.

142. Plaintiff and Class Members are "consumers," within the meaning of Civil Code Section 1761(d), because they are individuals who purchased products and/or services from Equifax.

143. Equifax performed "services," as defined by California Civil Code Section 1761(a), with respect to its compilation, maintenance, use, and furnishing of Plaintiff's and California Subclass members' PII that was compromised in the Data Breach.

144. Equifax's sale of their services to other consumers and businesses in California constitutes "transaction[s]" which were "intended to result or which result[ed] in the sale" of services to consumers within the meaning of Civil Code Sections 1761(e) and 1770(a).

145. Plaintiff has standing to pursue this claim as they have suffered injury in fact and have lost money as a result of Equifax's actions as set forth herein.

Specifically, Plaintiff's PII has been compromised and is imminently threatened with financial and identity theft, and, in fact, may have already suffered actual fraud.

146. Section 1770(a)(5) of the CLRA prohibits anyone from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have . . . ." Equifax represented that its credit background check services would adequately secure Plaintiffs' and California Subclass members' PII when in fact its computer systems were inadequately protected and susceptible to breach.

147. Section 1770(a)(7) of the CLRA prohibits anyone from "[r]epresenting that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another." Equifax represented that its credit background check services would adequately secure Plaintiff's and California Subclass members' PII when in fact its computer systems were inadequately protected and susceptible to breach.

148. Section 1770(a)(9) of the CLRA prohibits anyone from "[a]dvertising goods or services with intent not to sell them as advertised." As noted above, Equifax failed to provide adequate security to the PII it was entrusted to secure for the purposes of conducting credit background checks.

149. A written pre-suit demand under Cal. Civ. Code § 1782(a) is unnecessary and unwarranted because Equifax has long had notice of Plaintiff's allegations, claims and demands.

150. Plaintiff, individually and on behalf of the California Subclass, seek damages, an order enjoining the acts and practices described above, and attorneys' fees and costs under the CLRA.

RELIEF REQUESTED

Plaintiff, on behalf of himself 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 Class and Subclass requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is a proper representative of the Class and Subclass requested herein;

B. Injunctive relief requiring Equifax to (1) strengthen its data security systems that maintain PII to comply with the FCRA and GLBA, the applicable state laws alleged herein (including but not limited to the California Customer Records Act) and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Equifax'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 Equifax to pay all costs associated with Class notice and administration of Class-wide relief;

D. An award to Plaintiff and all Class (and Subclass) members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;

E. An award to Plaintiff and all Class (and Subclass) 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 Equifax 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.

Dated: September 9, 2017

Respectfully submitted,

ROBINSON CALCAGNIE, INC.

/s/ Daniel S. Robinson

Daniel S. Robinson
drobinson@robinsonfirm.com
19 Corporate Plaza Dr.
Newport Beach, CA 92660
Telephone: (949) 720-1288

Counsel for Plaintiffs and the Proposed Classes

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all issues in this action so triable of right.

Dated: September 9, 2017

Respectfully submitted,

ROBINSON CALCAGNIE, INC.

/s/ Daniel S. Robinson

Daniel S. Robinson
drobinson@robinsonfirm.com
19 Corporate Plaza Dr.
Newport Beach, CA 92660
Telephone: (949) 720-1288

Counsel for Plaintiffs and the Proposed Classes