BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
THOMAS J. O'REARDON II (247952)
JENNIFER L. MACPHERSON (202021)
701 B Street, Suite 1700
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
toreardon@bholaw.com
jmacpherson@bholaw.com

[Additional counsel appear on signature page]

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF CALIFORNIA

ANDREW DREMAK, on Behalf of Himself and All Others Similarly Situated,

Plaintiff,

v.

EQUIFAX, INC.,

Defendant.

Case No. '17CV1829 JM BGS

CLASS ACTION

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Andrew Dremak ("Plaintiff"), individually and on behalf of the general public and all others similarly situated (the "Class members"), by and through his attorney, upon personal knowledge as to facts pertaining to him and on information and belief as to all other matters, brings this action against Defendant Equifax, Inc. ("Equifax"), and respectfully states the following:

NATURE OF THE CASE

1. Equifax waited until September 7, 2017, to announce it experienced a massive data breach involving some of the most sensitive and private information from approximately 143 million U.S. consumers (the "Data Breach"). According to Equifax "[c]riminals 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." Equifax revealed the accessed information includes names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card and certain dispute documents with personal identifying information.

2. Equifax is a global giant in the business of maintaining and using private, sensitive consumer information. While primarily known as a consumer reporting agency, Equifax has expanded its information collection and dissemination services to include subscription-based credit monitoring and identity theft protection services for consumers and payroll and human resources services. According to Equifax it "organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide[.]"

3. As part of its business, Equifax collects and organizes personal private information about consumers, including Plaintiff and other Class members. Equifax obtains consumers' private information from the services it provides, as well as from credit card companies, banks, credit unions, retailers, auto and mortgage lenders, and other sources that provide personal private

information to Equifax and other credit reporting agencies. Equifax disseminates this information, which includes consumer credit scores, credit histories, and risk analysis to lenders, retailers, automotive dealers, and mortgage companies. This information determines an individual's creditworthiness, which can affect their ability to gain loans, housing and jobs.

4. Equifax also is in the business of selling credit and identity theft protection services to consumers; a highly lucrative business in which it makes many millions of dollars.

5. Plaintiff and the other Class members reasonably expect and believe that Equifax will take appropriate measures to protect their personally identifiable information ("PII"). Equifax informs customers that it will protect their PII. According to Equifax, it has "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."

6. Equifax assures consumers using its personal credit report service that it is "committed to protecting the security of your information through procedures and technology." Consumers of Equifax's personal products are told that Equifax is "committed to protecting the security of your personal information and use technical, administrative and physical security measures that comply with applicable federal and state laws."

7. Equifax's cybersecurity measures were so deficient that it took almost three months for it to discover that criminal hackers had gained access to Plaintiff's and Class members' PII.

8. Equifax owed a legal duty to Plaintiff and the other Class members to maintain reasonable and adequate security measures to secure, protect, and

safeguard the personal information stored on its network. Equifax breached that duty by failing to design and implement appropriate firewalls and computer systems, failing to properly and adequately encrypt data, and unnecessarily storing and retaining Plaintiff's and the other Class members' personal information on its inadequately protected network.

9. Equifax was aware of its inadequate cybersecurity before the Data Breach, yet failed to appropriately safeguard the PII. Before the Data Breach, Equifax's network had been hacked by criminals on numerous occasions. Nonetheless, Equifax failed to take reasonable measures to safeguard the PII and never warned Plaintiff and the other Class members that the information they provided to Equifax was unreasonably susceptible to hackers. To the contrary, Equifax promised it was adequately safeguarding consumers' PII.

10. As the result of Equifax's inadequate cybersecurity, the Data Breach occurred and Plaintiff's and the other Class members' PII was compromised and stolen, placing them at an increased risk of fraud and identity theft, and causing direct financial expenses associated with credit monitoring, replacement of compromised credit, debit and bank card numbers, and other measures needed to protect against fraud arising from the Data Breach.

11. This action seeks to remedy these failings. Plaintiff brings this action on behalf of himself and persons whose personal or financial information was disclosed as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

12. Plaintiff seeks, for himself and the Class, injunctive relief, actual and other economic damages, consequential damages, nominal damages or statutory damages, punitive damages, and attorneys' fees, litigation expenses and costs of suit.

VENUE AND JURISDICTION

13. This Court has subject matter jurisdiction over this action 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.

14. This Court has personal jurisdiction over Equifax because Equifax is authorized to conduct business in California, and does in fact conduct business in California. Equifax therefore has sufficient minimum contacts with the state to render exercise of jurisdiction by this Court in compliance with traditional notions of fair play and substantial justice.

15. Venue is proper in this judicial district pursuant to 28 U.S.C. §1391 because Equifax regularly conducts business in this district, unlawful acts or omissions are alleged to have occurred in this district, and Equifax is subject to personal jurisdiction in this district.

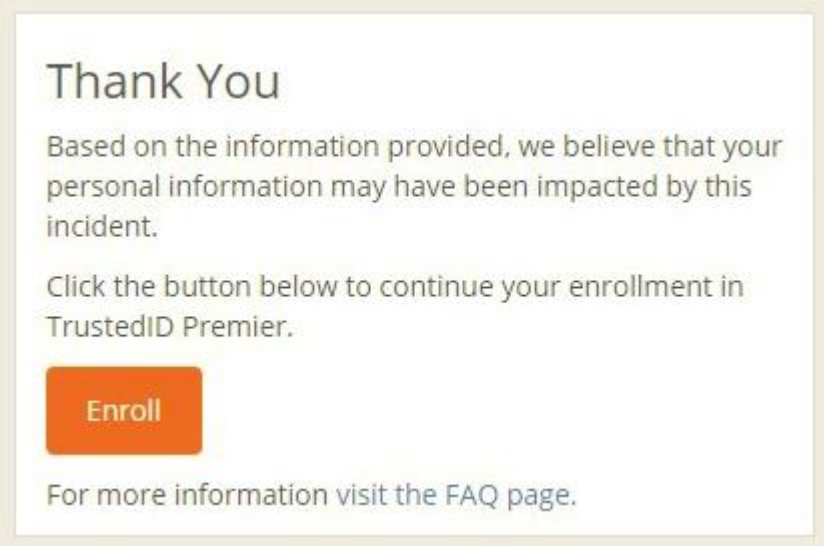
PARTIES

16. Plaintiff Andrew Dremak is an individual and a resident of San Diego, California. On information and believe, Mr. Dremak has provided Equifax with access to his confidential and highly sensitive personal and private information in connection with loan and credit applications. On September 8, 2017, Mr. Dremak visited Equifax's website, https://www.equifaxsecurity2017.com/, to check if his sensitive PII was stolen as a result of the Equifax Data Breach. After entering his last name and the last six digits of his social security number, Mr. Dremak received a prompt that stated his information "may have been impacted" by the Data Breach:

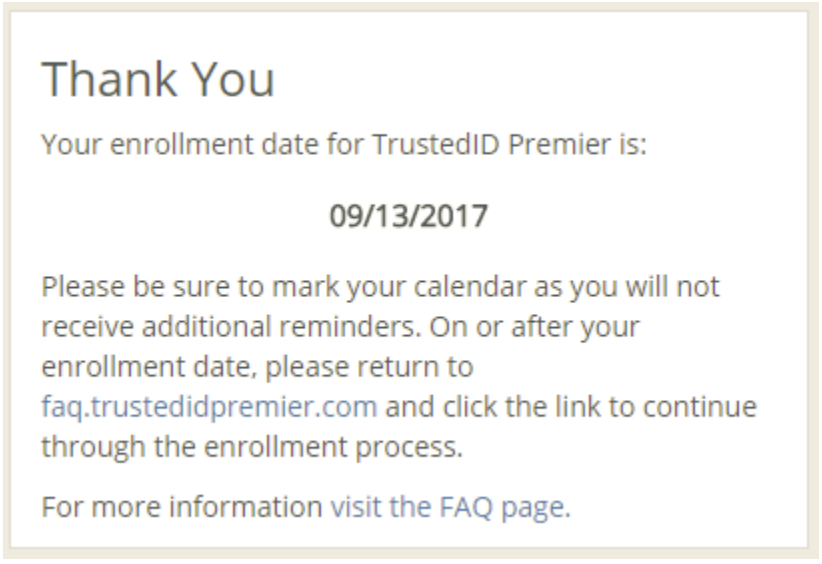
///

///

///



Concerned, and believing his PII was stolen and compromised, Mr. Dremak followed Equifax's instructions to enroll in TrustedID Premier monitoring services. However, after clicking "Enroll", Mr. Dremak was not able to enroll. Instead, he was simply provided a future "enrollment date" to sign up for Equifax's TrustedID Premier monitoring services, and informed to check back on the future date because he would not receive additional reminders:



17. Plaintiff Dremak's sensitive PII has been compromised and stolen as a result of the Data Breach and Equifax's unlawful conduct alleged herein. As a direct and proximate result of Equifax's wrongful actions, inaction and/or

omissions, the resulting Data Breach, and the resulting identity theft and identity fraud[1] inflicted on Plaintiff by one or more unauthorized third parties, Plaintiff also has suffered (and will continue to suffer) economic damages and other injury and harm in the form of the deprivation of the value of his PII, for which there is a well-established national and international market. PII is a valuable property right. Faced with the choice of having his PII disclosed, compromised, transferred, sold, opened, read, mined and otherwise used without his authorization versus selling his PII on the black market and receiving the compensation himself, Plaintiff would choose the latter. Plaintiff – not data thieves – should have the exclusive right to monetize his PII. Equifax's wrongful actions, inaction and omissions, and the resulting Data Breach, deprived him of this right.

18. As a further direct and proximate result of Equifax's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the resulting identity theft and identity fraud inflicted by one or more unauthorized third parties, Plaintiff has suffered (and will continue to suffer) other economic damages and injury and harm, including: (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud; (ii) invasion of privacy; (iii) breach of the confidentiality of his PII; (iv) deprivation of the value of his PII, for which there is a well-established national and international market; and/or (v) the financial and/or temporal cost of monitoring his credit, monitoring his financial accounts, and mitigating his damages – for which he is entitled to compensation.

[1] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia*, credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services, including medical services).

19. Defendant Equifax, Inc. is incorporated in Georgia, with its headquarters and principal place of business located at 1550 Peachtree Street, N.W., Atlanta, Georgia 30309. Equifax is a citizen of Georgia.

20. Equifax is one of the major credit reporting agencies in the United States. As a credit bureau service, Equifax is engaged in a number of credit-related services, as described by Equifax "[t]he company 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." As a credit reporting agency, Equifax maintains information related to the credit history of consumers and provides the information to credit grantors who are considering a borrower's application for credit or who have extended credit to the borrower.

FACTUAL ALLEGATIONS

Personal Identification Information Is a Valuable Property Right

21. At a Federal Trade Commission ("FTC") public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's PII:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy.
>
> Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[2]

22. Though Commissioner Swindle's remarks are more than a decade old, their pertinence has increased over time, as PII functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the

[2] Federal Trade Commission, *The Information Marketplace: Merging and Exchanging Consumer Data*, *Conference and Workshop*, *Washington D.C.*, 28 (March 13, 2011), *available at* https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

United States.[3]

23. The FTC has also recognized that PII is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[4]

24. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And by making the transaction transparent, consumers will make a profit from the surrender of their PI.[5] This business has created a new market for the sale and purchase of this valuable data.[6]

25. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and

---

[3] *See* J. Angwin and W. Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, Feb. 28, 2001, *available at* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

[4] Federal Trade Commission, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), (Dec. 7, 2009), *available at* https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[5] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times, July 16, 2010, *available at* http://www.nytimes.com/2010/07/18/business/18unboxed.html?_r=0.

[6] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal, Feb. 28, 2011, *available at* http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[7]

26. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII – the very injury at issue here – between $11.33 and $16.58 per website.[8]

27. The United States Government Accountability Office noted in a June, 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as SSNs to open financial accounts, receive government benefits and incur charges and credit in a person's name.[9] As the GAO Report states, this type of identity theft is the most harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

28. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."

29. According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[10] Identity thieves use personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and

---

[7] Janice Y. Tsai, *et al.*, *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* http://www.guanotronic.com/~serge/papers/isr10.pdf.

[8] II–Horn, Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.321.6125&rep=rep1&type=pdf (emphasis added).

[9] *See* http:///www.gao.gov/new.items/d07737.pdf.

[10] *See* FTC Identity Theft Website: www.ftc.gov/bcp/edu/microsites/idtheft/consumers /about-identity-theft.html.

bank/finance fraud.[11]

30. With access to an individual's sensitive information, criminals are capable of conducting many nefarious actions. Besides emptying the victim's bank account, identity thieves also commit various types of government fraud, such as: (1) obtaining a driver's license or official identification card in the victim's name but with the thief's picture; (2) using the victim's name and SSN to obtain government benefits; and/or (3) filing a fraudulent tax return using the victim's information.

31. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.[12]

32. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

33. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach,

---

[11] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR §603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[12] *See* FTC Identity Theft Website, *supra*.

that hackers released the stolen email and password combinations.[13]

34. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[14] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

35. Companies, in fact, also recognize PII and other sensitive information as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[15]

36. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII and other sensitive information directly on various Internet websites making the information publicly available. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list." The study concluded:

///

///

///

---

[13] *See* https://blog.linkedin.com/2016/05/18/protecting-our-members.

[14] *See* John T. Soma, *et al.*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (citations omitted).

[15] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[16]

37. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

38. It is within this context that Plaintiff and the 143 million Americans must now live with the knowledge that their personal information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Equifax Failed to Timely Disclose the Data Breach

39. On September 7, 2017, Equifax announced a massive Data Breach by criminals that gained access to files storing sensitive personal data for 143 million Americans, including names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and other PII.

40. According to Equifax, the hackers had access to the aforementioned sensitive, personal information of 143 million Americans from at least May 2017 until July 29, 2017, when the intrusion was discovered.

41. Equifax's preliminary investigation found the breach was due to its error – a vulnerability in an application in its U.S. website – which allowed hackers access to certain files.

42. While Equifax learned of the Data Breach on or before July 29, 2017, it waited for more than a month before informing the public. As of filing

[16] http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/

this complaint, Plaintiff and Class members affected by the Data Breach still have not been personally notified by Equifax.

43. The Gramm-Leach-Bliley Act ("GLBA") imposes upon "financial institutions", including credit reporting agencies such as Equifax, "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).

44. 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. §314.3.

45. Under the Interagency Guidelines Establishing Information Security Standards, 12 CFR Appendix D-2 to Part 208, 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 Supplement A, §II.

46. 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*. at Supplement A, §III.A.

47. "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.

48. 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: (a) Equifax's failure to implement and maintain adequate data security practices to safeguard Plaintiff's and Class members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendant's data security practices were inadequate to safeguard Plaintiff's and Class members' PII.

49. 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[.]" This includes, but is not limited to, Equifax's failure to notify the affected individuals themselves of the Data Breach in a timely and adequate manner.

Equifax's Belated Description of the Data Breach Is Inadequate and Misleading

50. As of September 8, 2017, more than one month since Equifax discovered the Data Breach, it still had not sent Plaintiff and Class members notice that their sensitive PII was compromised and stolen. Instead, as described herein, the belated public statements Equifax did make about the Data Breach are misleading, incomplete and fail to provide consumers with basic, important information about the scope and breadth of the stolen PII, and even whether their sensitive PII was accessed and stolen in the first place.

51. On September 7, 2017, Equifax issued a press release that hackers gained access to the most sensitive, private data of 143 million Americans. The release is materially misleading and does not disclose to consumers the full scope of the ongoing threat. For example, while the first line of Equifax's press release states "No Evidence of Unauthorized Access to Core Consumer or Commercial Credit Reporting Databases", the release goes on to state that names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and "certain dispute documents with personal identifying information" were accessed.

52. On September 7, 2017, Equifax set up a website where it instructed consumers to "determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection." The website, www.equifaxsecurity2017.com, is also misleading and does not provide material information to consumers. For example, on September 7, 2017, the website did not inform anyone that their PII had been impacted or potentially impacted. Instead, it merely instructed some consumers that they should check back at a future date to enroll in a "credit file monitoring and identity theft protection" product called TrustedID Premier. On September 8, 2017, it appears Equifax updated the information on its website to vaguely state for some consumers, such

as Plaintiff, that "Based on the information provided, we believe that your personal information *may* have been impacted by this incident."

53. Equifax's Data Breach press release and website also failed to explain the breadth of the Data Breach and the potential threat that consumers' face as a result of the sensitive PII being in the hands of criminals. For example, there are no specifics about how the breach occurred or why their consumer PII was not properly safeguarded and protected.

54. Many affected consumers will not see Equifax's press release or check if they were potentially impacted by visiting Equifax's website. Equifax could have sent text messages, like J.P. Morgan Chase and other banks use to instantly notify customer of a fraud alert of breach of their secured account, but instead chose to only issue a press release and set up a website.

55. Thus, Equifax's press release, its website for consumers to check for potential impact, and its other public statements about the Data Breach are misleading and do not adequately inform consumers whether their information was accessed and stolen, or what types of their information was accessed and stolen.

Equifax's Offer of Limited Credit Monitoring Is Inadequate and May Compromise Consumers' Rights

56. Equifax's Data Breach notices also squarely place the burden on Plaintiff and Class members, rather than Equifax, to protect themselves and mitigate their data breach damages. Equifax instructed its customers to review their account statements, monitor their credit reports, and obtain fraud alerts: "please monitor your account statements and report any unauthorized charges to your credit card companies and financial institutions" and "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."

57. Equifax's Data Breach notice states that Equifax will provide one year of credit monitoring and identity theft protection to U.S. consumers. The offered "credit monitoring," however, is inadequate and requires affected customers to spend additional time and resources to obtain full coverage. Moreover, Equifax is not actually providing the credit monitoring product at this time. Instead, even consumers whom Equifax believes may have been impacted are only provided a future date when they must return to Equifax's website to complete the process for signing up for TrustedID Premier. To make matters worse, unbeknownst to the reasonable consumer, to sign up for TrustedID Premier, Equifax purports to bind them to its "Terms of Use", which includes a mandatory arbitration provision and class action waiver.

58. The one-year credit monitoring offered by Equifax also does not provide comprehensive protection to the affected customers. Equifax does not disclose this important fact. For example, the limited one-year offer does not include monitoring the online black market for identity theft.

59. Equifax's Data Breach notices also states you may wish to place a "fraud alert" on your credit report. Equifax's Data Breach notices do not disclose the important fact that a fraud alert may not prevent the misuse of existing accounts, and for that reason the Federal Trade Commission still recommends "You still need to monitor all bank, credit card and insurance statements for fraudulent transactions."[17]

60. Equifax's Data Breach notice also states you may wish to place a "credit freeze" on your credit reports. As a general rule, the fee to place a "credit freeze" on one's credit report, as suggested by the Data Breach notice, is approximately $5-$10 each time it is placed at each of the three credit reporting agencies (Equifax, Experian and TransUnion). Thereafter, in order to allow anyone to check your credit, there is also an associated fee each time to lift the

[17] http://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

freeze. Moreover, if an identify thief has already used data to open accounts, then a credit freeze will not provide any benefits. A credit freeze also does not prevent identity thieves from making changes to existing accounts.

61. Monitoring one's credit reports, another option suggested by the Data Breach notice, would cause an affected consumer to incur an expense to see his or her credit reports beyond the one free annual report to which they are entitled.

Equifax Failed to Honor Its Promises to Keep Sensitive Personal Information Confidential

62. Equifax touts itself as an industry leader in data breach security and often promotes the importance of data breach prevention. Equifax offers services directly targeted to assisting consumers who have encountered a data breach. This includes credit-monitoring and identity-theft protection products to guard consumers' personal information.

63. Equifax describes itself as a "global information solutions company that uses ***trusted*** unique data, innovative analytics, technology and industry expertise to power organizations and individuals around the world by transforming knowledge into insights that help make more informed business and personal decisions."[18]

64. Equifax says that it "develop[s], maintain[s] and enhance[s] secured proprietary information databases through the compilation of consumer specific data, including credit, income, employment, asset, liquidity, net worth and spending activity, and business data, including credit and business demographics, that we obtain from a variety of sources, such as credit granting institutions, income and tax information primarily from large to mid-sized companies in the U.S., and survey-based marketing information. We process this information

[18] *See* http://www.equifax.com/about-equifax/company-profile/ (last visited September 8, 2017).

utilizing our proprietary information management systems. We also provide information, technology and services to support debt collections and recovery management."[19]

65. Equifax concedes that "[b]usinesses rely on us for consumer and business credit intelligence, credit portfolio management, fraud detection, decisioning technology, marketing tools, debt management and human resources-related services. We also offer a portfolio of products that enable individual consumers to manage their financial affairs and protect their identity."[20]

66. Although Equifax knows about the vulnerabilities of its online website applications and databases and lack of internal supervisory mechanisms, Equifax continued to represent and promise that consumers' personal and private information was safe and secure.

67. Equifax is well aware of the dangers of identity theft cautioning consumers that "[i]dentity theft is committed when someone steals your personal information – such as your name, Social Security number, and date of birth – typically to hijack your credit and use it to open up new credit accounts, take out loans in your name, or access your bank or retirement accounts. An identity thief can even use your personal information to steal your tax refunds, seek medical services, or commit crimes in your name."[21]

68. Equifax acknowledges that "[o]nce an identity thief has access to your personal information, he or she can also:

---

[19] *See* https://otp.tools.investis.com/clients/us/equifax/SEC/sec-show.aspx?Type=html&FilingId=12019947&Cik=0000033185 (last visited September 8, 2017).

[20] *See* file:///E:/BHO/Equifax/2016_annual_report.pdf (last visited September 8, 2017).

[21] *See* https://www.equifax.com/personal/education/identity-theft/what-is-identity-theft (last visited September 8, 2017).

- Open new credit card accounts with your name, Social Security number and date of birth. When the thief charges to the credit cards and leaves the bills unpaid, the delinquency will be reported to your credit report and could impact your credit score;

- Open a bank account in your name and write bad checks on the account;

- Create counterfeit checks or debit cards and use them to drain your existing bank accounts;

- File for bankruptcy under your name to avoid paying debts;

- Set up a phone, wireless, or other utility service in your name."

69. In articles and white papers regularly published by Equifax it recognizes the increasing risk of identity theft and the "Emotional Toll of Identity Theft" on victims.[22]

70. At all relevant times, Equifax designed and implemented its policies and procedures regarding the security of protected financial information and sensitive information. These policies and procedures failed to adhere to reasonable and best industry practices in safeguarding protected financial information and other sensitive information.

71. Plaintiff and Class members relied on Equifax to keep their sensitive information safeguarded and otherwise confidential.

72. Equifax's wrongful actions, inaction, omissions, and want of ordinary care in failing to completely and accurately notify Plaintiff and the

[22] *See* http://www.equifax.com/pdfs/corp/EFS-714-ADV_Predictive_Model_Fraud_WP_72409.pdf; https://www.equifax.com/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf; http://www.equifax.com/about-equifax/press-release-detail/en_gb?newsId=e7b7bb5b-dacb-4347-9747-8f73ac19d312; https://www.equifax.co.uk/data-breach/pdf/Identity%20Theft%20and%20Data%20Breach%20Whitepaper%2010-16_2.pdf (all last visited September 8, 2017).

Class about the Data Breach and corresponding unauthorized release and disclosure of their personal information was arbitrary, capricious and in derogation of Equifax's duties to Plaintiff and the Class.

CLASS ALLEGATIONS

73. Plaintiff brings this class action lawsuit on behalf of himself and all other members of the Class (the "National Class") defined as follows:

> All persons in the United States whose personal or financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

74. In the alternative to the National Class, Plaintiff seeks certification of a "Multistate Class" composed of statewide classes of persons from states with similar laws as applied to the facts of this case, or in the alternative, a California Class defined as follows:

> All persons in California whose personal or financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

75. The National Class, Multistate Class, and California Class are collectively referred to as the Class.

76. Excluded from the Class are: (1) Equifax and its officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

77. **Numerosity.** While the exact number of Class members is unknown, Equifax has admitted the personal information, including names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers of approximately 143 million Americans was taken during the Data Breach. Plaintiff therefore believes that the Class is so numerous that

joinder of all members is impractical.

78. **Typicality.** Plaintiff's claims are typical of the claims of the Class. Plaintiff and the Class members were injured by the same wrongful acts, practices, and omissions committed by Equifax, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

79. **Commonality.** Common questions of law and fact exist as to all Class members and predominate over any individual questions. Such common questions include, but are not limited to:

(a) Whether Equifax has engaged in unlawful, unfair or fraudulent business acts or practices;

(b) Whether Equifax has engaged in the wrongful conduct alleged herein;

(c) Whether Equifax used reasonable or industry standard measures to protect Class members' personal and financial information;

(d) Whether Equifax adequately or properly segregated its network so as to protect personal customer data;

(e) Whether Equifax knew or should have known prior to the security breach that its network was susceptible to a potential data breach;

(f) Whether Equifax should have notified the Class that it failed to use reasonable and best practices, safeguards, and data security measures to protect customers' personal and financial information;

(g) Whether Equifax should have notified Class members that their personal and financial information would be at risk of unauthorized disclosure;

(h) Whether Equifax intentionally failed to disclose material information regarding its security measures, the risk of data interception, and the Data Breach;

(i) Whether Equifax's acts, omissions, and nondisclosures were intended to deceive Class members;

(j) Whether Equifax's conduct violated the laws alleged;

(k) Whether Plaintiff and the Class members are entitled to restitution, disgorgement, and other equitable relief; and

(l) Whether Plaintiff and the Class members are entitled to recover actual damages, statutory damages, and punitive damages.

80. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that he has no interests which are adverse to or conflict with those of the Class members Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

81. **Superiority.** A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class may be relatively small. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION

Negligence

82. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

83. During the course of conducting its business, Equifax collected consumer's PII. It was reasonably foreseeable that third parties would attempt to acquire such information given the risk and frequency of security breaches at Equifax and highly publicized breaches elsewhere, including a May 2016 incident in which Equifax's W-2 Express website suffered an attack that resulted in the leak of PII from 430,000 persons, a breach between April 17, 2016 and March 29, 2017 to customers' employee tax records, a breach announced by Equifax in January 2017 in which credit information of customers at partner LifeLock had been exposed, a breach announced by Equifax to the New Hampshire attorney general in May 2014, prior security alerts, and the potential fraudulent and criminal uses of the information if acquired, among other things.

84. In addition, Equifax had notice of a possible security breach due to the prior targeting of other large retailers and financial institutions, including itself, by third parties seeking such information.

85. Consequently, Equifax as a consumer credit reporting agency, entrusted with the sensitive PII of over 800 million consumers and 88 million businesses worldwide, was trusted by its customers and other consumers to safeguard their personal and private information, including sensitive financial data such as credit card numbers. Equifax had a special duty to exercise reasonable care to protect and secure the PII so as to prevent its collection, theft, or misuse by third parties.

86. Equifax should have known to take precaution to secure consumers' PII, given its special duty.

87. Equifax likewise had a duty to exercise reasonable care under the circumstances to prevent any breach of security that would result in the loss, disclosure or compromise of the personal and financial information of Plaintiff and the Class, given its prior knowledge of security breaches.

88. Equifax also had a duty to exercise reasonable care under the circumstances to detect any breach of security that would result in the loss, disclosure or compromise of the personal and financial information of Plaintiff and the Class.

89. Once a security breach was detected, Equifax had a duty to exercise reasonable care under the circumstances to notify affected persons in order to minimize potential damage to Plaintiff and the Class due to the loss, disclosure or compromise of their personal and financial information.

90. Equifax breached its duty of care by failing to adequately secure and protect Plaintiff's and the Class members' personal and financial information from theft, collection and misuse by third parties.

91. Equifax further breached its duty of care by failing to promptly, clearly, accurately, and completely inform Plaintiff and the Class of the security breach.

92. Plaintiff's and Class members' PII was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated without their authorization as the direct and proximate result of Equifax's failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Class members' PII.

93. The policy of preventing future harm further weighs in favor of finding a special relationship between Equifax and the Class. Consumers count on Equifax to keep their personal information safe. If companies are not held

accountable for failing to take reasonable security measures to protect consumers' private and personal information, such as names, social security numbers, and contact information, they will not take the steps that are necessary to protect against future data breaches.

94. It was foreseeable that if Equifax did not take reasonable security measures, the data of Plaintiff and members of the Class would be taken.

95. Major credit reporting agencies like Equifax face a higher threat of security breaches than other types and sizes of businesses due in part to the scope and breadth of the personal, private, and sensitive information that Equifax possesses about hundreds of millions of consumers.

96. As a direct and proximate result of Equifax's conduct and breach of its duties, Plaintiff and the Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII, for which there is a well-established national and international market, (v) failure to receive the full benefit of their bargain as a result of receiving credit fraud and monitoring services that were less valuable than what they paid for, and/or (vi) the financial and/or temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

97. Neither Plaintiff nor other members of the Class contributed to the security breach, nor did they contribute to Equifax's employment of insufficient security measures to safeguard consumers' PII, including Social Security numbers and debit and credit card information.

98. Plaintiff and the Class seek compensatory damages and punitive damages with interest, the costs of suit and attorneys' fees, and other and further relief as this Court deems just and proper.

99. Equifax's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach constitute common law negligence, gross negligence, and negligence *per se*.

SECOND CAUSE OF ACTION

Violations of the California Customer Records Act (Civil Code §1798.80, *et seq*.)

100. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

101. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted the Customer Records Act (the "California CRA"), Civil Code §1798.81.5, which requires that any business that "owns licenses, or maintains personal information about a California resident shall 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."

102. The events alleged herein constituted a "breach of the security system" of Equifax within the meaning of Civil Code §1798.82.

103. The information lost, disclosed, or intercepted during the events alleged herein constituted unencrypted "personal information" within the meaning of Civil Code §§1798.80(e) and 1798.82(h).

104. Equifax failed to implement and maintain reasonable or appropriate security procedures and practices to protect consumers' personal and financial information. On information and belief, Equifax failed to employ industry standard security measures, best practices or safeguards with respect to consumers' personal and financial information.

105. Equifax failed to disclose the breach of security of its system in the most expedient time possible and without unreasonable delay after it knew or

reasonably believed that consumers' personal information had been compromised.

106. The breach of the personal information of millions of Equifax's consumers' records constituted a "breach of the security system" of Equifax pursuant to Civil Code §1798.82(g).

107. By failing to implement reasonable measures to protect consumers' personal data it maintained, Equifax violated Civil Code §1798.81.5.

108. In addition, by failing to promptly notify all affected consumers that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, Equifax violated Civil Code §1798.82 of the same title in a manner that would reach all affected consumers.

109. By violating Civil Code §§1798.81.5 and 1798.82, Equifax "may be enjoined" under Civil Code §1798.84(e).

110. Accordingly, Plaintiff requests that the Court enter an injunction requiring Equifax to implement and maintain reasonable security procedures to protect consumers' data in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Equifax, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis; (2) ordering that Equifax engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Equifax, consistent with industry standard practices, conduct regular database scanning and security checks; (5) ordering that Equifax, consistent with industry standard practices, periodically conduct internal training and education to inform internal

security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (6) ordering Equifax to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

111. Plaintiff further requests that the Court require Equifax to: (1) identify and notify all members of the Class who have not yet been informed of the data breach; and (2) to notify affected customers of any future data breaches by email and text within 24 hours of Equifax's discovery of a breach or possible breach, and by mail within 72 hours.

112. As a result of Equifax's violation of Civil Code §§1798.81, 1798.81.5, and 1798.82, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII, for which there is a well-established national and international market, (v) failure to receive the full benefit of their bargain as a result of receiving credit fraud and monitoring services that were less valuable than what they paid for; and/or (vi) the financial and/or temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

113. Plaintiff, individually and on behalf of the members of the Class, seeks all remedies available under Civil Code §1798.84, including, but not limited to: (a) damages suffered by members of the Class; and (b) equitable relief. Plaintiff, individually and on behalf of the members of the Class, also seeks reasonable attorneys' fees and costs under applicable law.

THIRD CAUSE OF ACTION

Violations of the California Unfair Competition Law (Bus. & Prof. Code §17200, *et seq.*)

114. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

115. The California Unfair Competition Law, Bus. & Prof. Code §17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of its above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Equifax engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

116. In the course of conducting its business, Equifax committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' PII, and violating the statutory and common law alleged herein in the process, including, *inter alia,* California's Customer Records Act (Civ. Code §1798.80, *et seq.*), California's UCL, California's CLRA, the Gramm-Leach-Bliley Act, and common law negligence. Plaintiff and Class members reserve the right to allege other violations of law by Equifax constituting other unlawful business acts or practices. Equifax's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

117. Equifax also violated the UCL by failing to timely notify Plaintiff and Class members regarding the unauthorized release and disclosure of their PII.

118. Equifax's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Equifax's wrongful conduct is substantially injurious to consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous. California has a well-defined public policy embodied by various states statutes, including California's Customer Records Act and Information Practices Act to ensure that businesses that maintain customer's personal information implement and maintain reasonable security procedures and practices to protect the personal information from unauthorized access, destruction, use, modification or disclosure. The gravity of Equifax's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Equifax's legitimate business interests other than engaging in the above-described wrongful conduct.

119. The UCL also prohibits any "fraudulent business act or practice." Equifax's above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

120. As a direct and proximate result of Equifax's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII, for which there is a well-established national and international market, (v) failure to receive the full benefit of their bargain as a result of receiving credit fraud and monitoring services that were

less valuable than what they paid for, and/or (vi) the financial and/or temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

121. Unless restrained and enjoined, Equifax will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of himself, Class members, and the general public, also seeks restitution and an injunction prohibiting Equifax from continuing such wrongful conduct, and requiring Equifax to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code §17203.

FOURTH CAUSE OF ACTION

Violations of the Consumers Legal Remedies Act (Civil Code § 1750, *et seq.*)

122. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

123. This cause of action is brought pursuant to the Consumers Legal Remedies Act, California Civil Code §1750, *et seq*. (the "Act") and similar laws in other states. Plaintiff is a consumer as defined by California Civil Code §1761(d). Equifax's TrustedID Premier Credit Monitoring & Identity Theft Protection is a "good" within the meaning of the Act.

124. Equifax violated and continues to violate the Act by engaging in the following practices proscribed by California Civil Code §1770(a)(19) ("Inserting an unconscionable provision in the contract") in transactions with Plaintiff and the Class which were intended to result in, and did result in, the sale of its TrustedID Premier products.

125. Equifax violated the Act by inserting an unconscionable provision in the contract for the TrustedID Premier monitoring product it offers Plaintiff, Class members and other consumers through the Data Breach. Buried within the fine-print adhesionary "Terms of Use" that accompany the TrustedID Premier product (and all products offered by Equifax) are purportedly mandatory binding arbitration and class action waiver provisions. Members of the Class do not reasonably know that they are potentially giving up valuable legal rights by accepting Equifax's post-breach offer of the limited credit monitoring product. On the other hand, Equifax, the drafter of the adhesionary provision and the party with superior bargaining power, receives unfairly one-sided benefits.

126. Pursuant to California Civil Code §1782(d), Plaintiff, individually and on behalf of the other members of the Class, seeks a Court order enjoining the above-described wrongful acts and practices of Equifax and for restitution and disgorgement.

127. Pursuant to §1782 of the Act, Plaintiff notified Equifax in writing by certified mail of the particular violations of §1770 of the Act, and demanded that Equifax rectify the problems associated with the actions detailed above and give notice to all affected consumers of Equifax's intent to so act. A copy of the letter is attached hereto as Exhibit A.

128. If Equifax fails to rectify or agree to rectify the problems associated with the actions detailed above and give notice to all affected consumers within 30 days of the date of written notice pursuant to §1782 of the Act, Plaintiff will amend this complaint to add claims for actual, punitive and statutory damages, as appropriate.

129. Equifax's conduct is fraudulent, wanton, and malicious.

130. Pursuant to §1780(d) of the Act, attached hereto as Exhibit B is the affidavit showing that this action has been commenced in the proper forum.

FIFTH CAUSE OF ACTION

Declaratory Relief

131. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

132. An actual controversy has arisen in the wake of the Data Breach regarding Equifax's duties to safeguard and protect Plaintiff's and Class members' confidential and sensitive PII. Equifax's PII security measures were (and continue to be) woefully inadequate. Equifax disputes these contentions and contends that its security measures are appropriate.

133. Plaintiff and Class members continue to suffer damages, other injury or harm as additional identity and financial theft and fraud occurs.

134. Therefore, Plaintiff and Class members request a judicial determination of their rights and duties, and ask the Court to enter a judgment declaring, *inter alia*, (i) Equifax owed (and continues to owe) a legal duty to safeguard and protect Plaintiff's and Class members' confidential and sensitive PII, and timely notify them about the Data Breach, (ii) Equifax breached (and continues to breach) such legal duties by failing to safeguard and protect Plaintiff's and Class members' confidential and sensitive PII, and (iii) Equifax's breach of its legal duties directly and proximately caused the Data Breach, and the resulting damages, injury, or harm suffered by Plaintiff and Class members. A declaration from the Court ordering Equifax to stop its illegal practices is required. Plaintiff and Class members will otherwise continue to suffer harm as alleged above.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all persons and consumers similarly situated, prays for judgment as follows:

A. An Order certifying the proposed Class defined herein, designating Plaintiff as representative of said Class, and appointing the

undersigned counsel as Class Counsel;

B. For restitution of all amounts obtained by Equifax as a result of its wrongful conduct in an amount according to proof at trial, plus pre-judgment and post-judgment interest thereon;

C. For all recoverable compensatory, consequential, actual, and/or statutory damages in the maximum amount permitted by law;

D. For punitive and exemplary damages;

E. For other equitable relief;

F. For such injunctive relief, declaratory relief, orders, or judgment as necessary or appropriate to prevent these acts and practices;

G. For payment of attorneys' fees and costs of suit as allowable by law; and

H. For all such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all issues so triable.

Respectfully submitted,

Dated: September 8, 2017

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
THOMAS J. O'REARDON II (247952)
JENNIFER L. MACPHERSON (202021)

By: *s/ Timothy G. Blood*
TIMOTHY G. BLOOD

701 B Street, Suite 1700
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
toreardon@bholaw.com
jmacpherson@bholaw.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW
ERICH P. SCHORK
1 North LaSalle Street, Suite 4600

Chicago, IL 60602
Tel: 312/621-2000
312/641-5504 (fax)
b.barnow@barnowlaw.com
e.schork@barnowlaw.com

THE COFFMAN LAW FIRM
RICHARD L. COFFMAN
First City Building
505 Orleans St., Fifth Floor
Beaumont, TX 77701
Tel: 409/833-7700
866/835-8250 (fax)
rcoffman@coffmanlawfirm.com

Attorneys for Plaintiff

JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
ANDREW DREMAK, on Behalf of Himself and All Others Similarly Situated

DEFENDANTS
EQUIFAX, INC.

(b) County of Residence of First Listed Plaintiff San Diego County, CA
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Timothy G. Blood/Thomas J. O'Reardon II/Jennifer L. MacPherson
Blood Hurst & O'Reardon, LLP
701 B Street, Ste. 1700, San Diego, CA 92101 Tel: 619/338-1100

Attorneys *(If Known)*

'17CV1829 JM BGS

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

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

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

Click here for: Nature of Suit Code Descriptions.

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

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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

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

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

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

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
28 U.S.C. §1332(d) (Diversity)

Brief description of cause:
Violations of: Civ. Code §1798.80 (Consumer Records Act); B&P Code §17200 (UCL); Civ. Code §1750 (CLRA)

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions):*

JUDGE _____ DOCKET NUMBER _____

DATE 09/08/2017

SIGNATURE OF ATTORNEY OF RECORD s/ Timothy G. Blood

FOR OFFICE USE ONLY

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

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

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

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

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

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

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

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

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

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

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

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

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

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

Exhibit A

BLOOD HURST & O'REARDON | LLP

701 B Street, Suite 1700 | San Diego, CA 92101
T | 619.338.1100 F | 619.338.1101
www.bholaw.com

Timothy G. Blood
tblood@bholaw.com

September 8, 2017

VIA CERTIFIED MAIL (RETURN RECEIPT)
(RECEIPT NO. 7014 0150 0000 6250 7437)

Richard F. Smith, Chairman and CEO
Equifax, Inc.
1550 Peachtree Street, NW
Atlanta, GA 30309

Re: Equifax Data Breach Lawsuit Demand Letter

Dear Mr. Smith:

We represent Andrew Dremak (collectively "Plaintiff") and all other consumers similarly situated in an action against Equifax, Inc. ("Defendant"), arising out of, *inter alia*, Equifax's failure to adequately safeguard certain financial, personal identification, and related data belonging to Plaintiff and others similarly situated. This information is collected and maintained by Equifax.

More specifically, Defendant failed to adequately secure consumers' personally identifiable information ("PII"), including names, Social Security numbers, birth dates, addresses driver's license numbers, credit card numbers, and certain dispute documents. Defendant was aware of this security breach, but withheld information about and/or failed to timely notify Plaintiff and others of the unauthorized third party access to their PII. The full claims, including the facts and circumstances surrounding these claims, are detailed in the Class Action Complaint, a copy of which is attached and incorporated by this reference.

Equifax represents itself as a leader in data security and agreed to and had a duty to, among other things, properly maintain Plaintiff's and Class members' PII. Defendant's conduct, including its representations and omissions regarding data security are false and misleading and constitute unfair methods of competition and unlawful, unfair, and fraudulent acts or practices.

Defendant's practices constitute violations of the California Consumers Legal Remedies Act, Civil Code §1750, *et seq*. Specifically, Defendant's practices violate Civil Code §1770(a) under, *inter alia*, the following subdivisions:

(19) Inserting an unconscionable provision in the contract.

As detailed in the attached Complaint, Defendant's practices also violate the California Consumer Records Act, Civil Code §1798.80, *et seq*., the California Unfair Competition Law, Bus. & Prof. Code §17200, *et seq*., and constitute negligence.

BLOOD HURST & O'REARDON | LLP

While the Complaint constitutes sufficient notice of the claims asserted, pursuant to California Civil Code §1782 we hereby demand on behalf of our client and all others similarly situated that Defendant immediately correct and rectify these violations by stopping the concealment of material information about the data breach and the release of Class members' PII, ceasing dissemination of false and misleading information as described in the enclosed Complaint, and initiating a corrective notice campaign that informs Class members of the nature of the data breach, the data released, and all corrective measures put in place to prevent any such breaches. In addition, Defendant must offer to not only monitor the credit of Plaintiff and all Class members, but also provide refunds for any damages, statutory or otherwise, plus provide reimbursement for interest, costs, and fees.

We await your response.

Sincerely,

FOR

TIMOTHY G. BLOOD

TGB:jk

Enclosure

Exhibit B

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
THOMAS J. O'REARDON II (247952)
JENNIFER L. MACPHERSON (202021)
701 B Street, Suite 1700
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
toreardon@bholaw.com
jmacpherson@bholaw.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF CALIFORNIA

ANDREW DREMAK, on Behalf of Himself and All Others Similarly Situated, Plaintiff, v. EQUIFAX, INC., Defendant.	Case No. **CLASS ACTION** **AFFIDAVIT OF TIMOTHY G. BLOOD PURSUANT TO CALIFORNIA CIVIL CODE §1780(d)** **DEMAND FOR JURY TRIAL**

I, TIMOTHY G. BLOOD, declare as follows:

1. I am an attorney duly licensed to practice before all of the courts of the State of California. I am the managing partner of the law firm of Blood, Hurst & O'Reardon, LLP, one of the counsel of record for Plaintiff Andrew Dremak in the above-entitled action.

2. Defendant Equifax, Inc. has done and is doing business in San Diego County, California. Such businesses include the provision of credit reports, as well as credit score subscription services, and credit monitoring identity theft subscription services, among others. Plaintiff is a resident of San Diego County, California.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed on September 8, 2017, at San Diego, California.

s/ Timothy G. Blood

TIMOTHY G. BLOOD