William T. Payne (CSB 90988)
Joseph N. Kravec, Jr.
(to be admitted *pro hac vice*)
FEINSTEIN DOYLE
PAYNE & KRAVEC, LLC
Law & Finance Building, Suite 1300
429 Fourth Avenue
Pittsburgh, PA 15219-1639
Tel: (412) 281-8400
Fax: (412) 281-1007
Email: wpayne@fdpklaw.com
Email: jkravec@fdpklaw.com

ATTORNEYS FOR PLAINTIFF
AND THE PROPOSED CLASS AND SUBCLASS

IN THE UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF CALIFORNIA

ALBERT LOUIS FRIED, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

EQUIFAX, INC., a Georgia corporation, and DOES 1-100,

Defendants.

Case No.: **'17CV1955 CAB KSC**

CLASS ACTION COMPLAINT FOR:

(1) Willful Violation of the Fair Credit Reporting Act
(2) Negligent Violation of the Fair Credit Reporting Act
(3) Negligence
(4) Negligence Per Se
(5) Constructive Fraud
(6) Violation of California's Data Breach Law (Cal Civ. Code §§ 1798.80 *et seq.*) and
(7) Violation of California's Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200, *et seq.*).

DEMAND FOR JURY TRIAL

Plaintiff Albert Louis Fried ("Plaintiff") by his attorneys, brings this class action on his own behalf and on behalf of all others similarly situated ("Class Members") against Defendant Equifax, Inc. ("Equifax"), and other unknown DOE Defendants (collectively all Defendants are referred to as "Defendant"), and alleges as follows upon information and belief based on, *inter alia*, the investigation of his counsel:

I. INTRODUCTION

1. This is a data breach class action on behalf of some 143 million consumers whose personal identifying information ("PII") including dates of birth, names, addresses, Social Security numbers ("SSNs"), driver's license numbers, and other personal information (collectively, "Data") was taken from Equifax in a cyber-attack that was first publically announced by Equifax on September 7, 2017 ("Data Breach").

2. Equifax is one of the three largest credit reporting agencies in the United States. It maintains highly sensitive personal identifying information for most Americans, and its credit reports are relied upon by American consumers and businesses alike for the extension of credit in the United States.

3. Equifax touts itself as an industry leader in managing and protecting data. Indeed, Equifax boasts:

> 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.[1]

4. Thus, Equifax was (or should have been) well aware of the importance of the measures organizations should take to prevent data breaches, including the

[1] http://www.equifax.com/privacy/ (last accessed September 21, 2017).

importance of promptly updating its systems to address vulnerabilities as they become disclosed, and willingly failed to take them.

5. According to Equifax's September 7, 2017 announcement of the Data Breach, the breach occurred "from mid-May through July 2017" as a result of a "website application vulnerability" that was "exploited" and permitted access, among other things, to "names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers." Equifax also noted that "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."[2]

6. Equifax has included a timeline of the breach on its website, including the following:

- On July 29, 2017, Equifax's Security team observed suspicious network traffic associated with its U.S. online dispute portal web application. In response, the Security team investigated and blocked the suspicious traffic that was identified.
- The Security team continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, the company took offline the affected web application that day.
- The company's internal review of the incident continued. Upon discovering a vulnerability in the Apache Struts web application framework as the initial attack vector, Equifax patched the affected web application before bringing it back online.[3]

7. Equifax claimed that "[t]he attack vector used in this incident occurred through a vulnerability in Apache Struts… an open-source application framework that supports the Equifax online dispute portal web application," and provided additional information regarding Apache Struts:

Questions Regarding Apache Struts

- The attack vector used in this incident occurred through a vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application.

---

[2] https://www.equifaxsecurity2017.com/ (last accessed September 21, 2017).

[3] *Id.*

- Based on the company's investigation, Equifax believes the unauthorized accesses to certain files containing personal information occurred from May 13 through July 30, 2017.
- The particular vulnerability in Apache Struts was identified and disclosed by U.S. CERT in early March 2017.
- Equifax's Security organization was aware of this vulnerability at that time, and took efforts to identify and to patch any vulnerable systems in the company's IT infrastructure.
- While Equifax fully understands the intense focus on patching efforts, the company's review of the facts is still ongoing. The company will release additional information when available.[4]

8. Equifax's confirmation that the Data Breach involved the Apache Struts vulnerability which was disclosed more than 2 months before the breach, revealed a simple truth: the breach could have been prevented had Equifax taken simple precautions to prevent the vulnerability:

> Capping a week of incompetence, failures, and general shady behavior in responding to its massive data breach, Equifax has confirmed that attackers entered its system in mid-May through a web-application vulnerability that had a patch available in March. In other words, the credit-reporting giant had more than two months to take precautions that would have defended the personal data of 143 million people from being exposed. It didn't.[5]

9. Equifax has not indicated that the Data which was disclosed during the Data Breach was encrypted. "[N]otably absent from the public statements by Equifax have been key terms such as 'encryption' or 'system monitoring' or 'penetration testing,'" which are "staples of modern online security widely adopted across corporate America and especially within the financial services industry, given the high degree of sensitivity about the information it keeps on us all." Additionally,

---

[4] *Id.*

[5] https://www.wired.com/story/equifax-breach-no-excuse/ (dated September 14, 2017, last accessed September 21, 2017).

"Equifax has not responded to repeated Washington Post requests about the nature of its security measures and whether any of its data was kept in encrypted form."[6]

10. Andrew Lewman, vice president of Owl Cybersecurity,

> said that if the Equifax data was encrypted, it would be much more difficult for hackers to use the personal data. But if Equifax had encrypted the data, it probably would have said so. "The stuff that's heavily encrypted, there's little value to it. It's like I have this secret box of stuff, and trust me it's gold, not coal," said Lewman.[7]

11. Thus, despite Equifax's professed expertise in the area of data protection, management and customer support, its lapse in security permitting the Data Breach and its response to this breach has been inadequate.

12. Equifax failed to adequately safeguard consumers' PII because it lacked or knowingly failed to take reasonable or proper safeguards to maintain security of Plaintiff's and Class Members' PII. Equifax's lack of reasonable security provided a means for unauthorized intruders to access Equifax's computer network and take consumers' sensitive PII.

13. Consumers could face a "lifelong battle" to deal with the consequences of Equifax's failure to secure their PII, including the filing of fraudulent tax returns, unauthorized loans or credit cards, and variety of other identity frauds. Equifax's failure to adequately protect customers' PII has caused, and will continue to cause, substantial harm and injuries to some 143 million customers affected across the United States.

14. Equifax delayed nearly 6 weeks after it learned of the breach on July 29, 2017 before it issued a press release on September 7, 2017 generically stating it had a breach affecting some 143 million customers. While that delay gave Equifax's top

---

[6] https://www.washingtonpost.com/news/the-switch/wp/2017/09/12/the-three-big-questions-equifax-hasnt-answered/?utm_term=.fe2cba0d7a7c (dated September 12, 2017, last accessed September 21, 2017).

[7] http://www.denverpost.com/2017/09/08/equifax-data-breach-what-happened/ (dated September 8, 2017, last accessed September 21, 2017).

executives time to dump their company stock before its price dropped[8], the notice on September 7, 2017 did not tell any specific person if their data was taken and, if so, which of their data was taken.

15. Despite the fact that around 143 million customers had PII that was accessed as a result of the Data Breach, according to their September 7, 2017 announcement, Equifax is only planning to "send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted."[9] That is a few hundred thousand out of 143 million people, constituting less than 0.3% of those affected by the breach.

16. Equifax has email addresses for a substantial portion of the 143 million affected customers. Indeed, Equifax requests or requires an email address be provided to it under a variety of situations, including when a consumer requests his or his own credit report, files a dispute or purchases one of the many services it sells.[10] At a minimum, Equifax should, and under many state laws (including California) is required to, provide notice of the breach to affected persons for whom it has email addresses. *See* Cal. Civ. Code 1798.82(j)(3)(A).

17. With regard to Plaintiff Fried, he provided Defendant with his email address approximately two years ago when he requested a credit report from Equifax, which was sent to his email address.

18. Rather than provide the direct notice it is required to provide to Plaintiff Fried and others, Equifax's September 7, 2017 announcement indicates that it has "established a dedicated website, www.equifaxsecurity2017.com, to help consumers

---

[8] https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack (dated September 7, 2017, updated September 8, 2017, last accessed September 21, 2017).

[9] https://www.equifaxsecurity2017.com/ (last accessed September 21, 2017).

[10] See Exhibits 1 and 2 (Forms showing that Equifax requests an email address when individuals request an Equifax Credit Report and Score or a Research Request).

determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection."[11] Equifax's website requires people to type in more personal information (*i.e.*, last name and six digits of one's social security number) to find out only if the individual may be affected, without providing any further details about what of their information was taken. Understandably, many customers may well be reluctant to provide more PII electronically to Equifax given its clear failure to safeguard the PII it already has. This is an unlawful and inadequate form of substitute notice.

19. A check of Equifax's dedicated breach website for Plaintiff on September 13, 2017 indicated that "we believe that your personal information may have been impacted by this incident." Prior to this check of Equifax's website, Plaintiff received no direct notice by U.S. mail, email or otherwise from Equifax notifying him that his PII was impacted by the Data Breach, nor has Equifax told Plaintiff which of his PII was taken.

20. Armed with the sensitive information obtained through the breach, data thieves can incur fraudulent debts; open new financial or utility accounts in a victim's name; use the victim's information to obtain government benefits; file fraudulent tax return using the victim's information to obtain a tax refund; obtain a driver's license or identification card in the victim's name but with another person's picture; and give false information to police during an arrest, amongst other things.

21. As a result of the breach, Plaintiff and Class Members (as defined below) are exposed to a heightened and imminent risk of fraud and identity theft and must now closely monitor their financial accounts to guard against identity theft well into the future. As a result, Plaintiff and Class Members may be faced with fraudulent debt, and incur out-of-pocket costs for, among other things, obtaining credit reports, credit freezes, or other protective measures to deter and detect identity theft.

---

[11] https://www.equifaxsecurity2017.com/ (last accessed September 21, 2017).

22. Plaintiff seeks to remedy these harms on behalf of himself and all similarly-situated individuals whose personal information was accessed during the breach.

23. Plaintiff seeks remedies on behalf of himself and millions of Equifax's customers throughout the United States who had their PII taken due to Equifax's failure to secure its computer systems, including but not limited to, restitution, damages, punitive damages, statutory damages under the Fair Credit Reporting Act ("FCRA"), reimbursement of out-of-pocket losses, further credit monitoring services with accompanying identity theft insurance, improved data security, and to compel immediate notice to affected persons advising they are affected by the data breach and what of their data was taken.

II. PARTIES

24. Plaintiff Albert Louis Fried is a natural person and a citizen of the State of California, residing in San Diego County.

25. Following the instructions set forth on the equifaxsecurity2017.com website, Plaintiff's last name and last six digits of his Social Security number were entered on the website on September 13, 2017. In response, a message was received indicating "[b]ased on the information provided, we believe that your personal information may have been impacted by this incident. Click the button below to continue your enrollment in TrustedID Premier." Plaintiff did not sign up for TrustedID Premier because he was concerned that the arbitration clause and class action waiver may be used to limit his rights to relief for the Data Breach.

26. Defendant Equifax is a Georgia corporation whose principal office address is 1550 Peachtree Street NW, Atlanta, GA, 30309-2402. Defendant is a credit reporting agency.

27. There are also unknown DOE Defendants in this case, consistent with Rule 474 of the California Rules of Civil Procedure.

III. JURISDICTION AND VENUE

28. This Court has federal question jurisdiction under 28 U.S.C. § 1331 because claims are brought under the federal Fair Credit Reporting Act, 15 U.S.C. §§ 1681e, *et seq*.

29. Jurisdiction of this Court also is proper under 28 U.S.C. § 1332(d)(2). The matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, and is a class action in which members of the class of plaintiffs are citizens of states different from Defendant.

30. Venue is proper within this judicial district pursuant to 28 U.S.C. §1391(b) and (c). Defendant transacts business and is found within this District, and a substantial portion of the underlying transactions and events complained of by the enterprise occurred in this district, and affected persons, including Plaintiff, reside or resided in this judicial district at the material time. Defendant has received substantial compensation from such transactions and business activity in this District.

IV. FACTUAL ALLEGATIONS

31. Credit reporting agencies, like Equifax, are in the business of collecting customers' personal and financial information and keeping it private and secured.

32. Credit reporting agencies, such as Equifax, know or should know of the risk that their customers' PII can be stolen and of the need to carefully safeguard this information, including the importance of promptly updating its systems to address security vulnerabilities as they become disclosed.

Equifax – Data Protection, Management and Customer Support Experts

33. Equifax touts 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.[12]

[12] https://www.equifaxsecurity2017.com/ (last accessed September 21, 2017).

34. Equifax's website boasts

> 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.[13]

35. Equifax's website also indicates that its

> data assets, technology and analytics transform knowledge into insights that power better decisions. This knowledge enables our customers to make better business decisions and consumers to progress towards a better life. We serve as a consumer advocate, steward of financial literacy, and champion of economic advancement.[14]

36. On that website, Richard F. Smith, Equifax's former Chairman and CEO, is quoted as saying

> Equifax helps people make better decisions by weaving unique data and insights into knowledge that makes a difference. Our strategic focus has stood the test of time and allowed us to evolve into a better, more sophisticated partner for our customers, consumers, and shareholders. No longer just a consumer credit company, we are a global insights powerhouse driven by innovation, adherence to our core values, and the best talent in the industry.[15]

Equifax – Past Data Breaches

37. Equifax has experienced data breaches in the past, as detailed in an article by Thomas Fox-Brewster on forbes.com entitled "A Brief History of Equifax Security Fails." That article mentioned various data breaches at Equifax over the past few years, including:

> •A class action lawsuit filed regarding "a May 2016 incident in which Equifax's W-2 Express website had suffered an attack that resulted in the leak of 430,000 names, addresses, social security numbers and other personal information of retail firm Kroger. Lawyers for the class action plaintiffs argued Equifax had 'wilfully ignored known weaknesses in its data security, including prior hacks into its information systems.'… In the end, the case was dropped without

---

[13] http://www.equifax.com/privacy/ (last accessed September 21, 2017).

[14] http://www.equifax.com/about-equifax/ (last accessed September 21, 2017).

[15] *Id.*

> prejudice (i.e. the claims could be brought again), with the stipulation that Equifax fix a glaring security issue" regarding PIN numbers.
>
> •However, the article notes "problems with PINs appeared to have continued after that settlement in September last year. As independent cybersecurity reporter Brian Krebs reported in May 2017 an Equifax note to customers that hackers had used personal information to guess personal questions of employees in order to reset the 4-digit PIN given and stolen tax data. In its disclosure, Equifax said the unauthorized access to the information occurred between April 17 2016 and March 29 the following year."
>
> •Additionally, "[i]n January 2017, Equifax was forced to confess to a data leak in which credit information of a 'small number' of customers at partner LifeLock had been exposed to another user of the latter's online portal."
>
> •Finally, the article notes that "Equifax reported to the New Hampshire attorney general of a breach, admitting that between April 2013 and January 2014, an 'IP address operator was able to obtain the credit reports using sufficient personal information to meet Equifax's identity verification process.' There were other smaller data leaks reported by Equifax to the AG, though they only appeared to affect a handful of people." [16]

38. That article also noted that there are serious questions about Equifax's security procedures, at least one of which was raised even before the latest data breach. It further noted that

> good-guy hackers have found myriad old technologies running the Equifax site, many of which could be vulnerable to cyberattack. Researcher Kenneth White 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 pro who's spent 17 years helping protect businesses, found decade-old software in use.[17]

39. Equifax, by virtue of its alleged expertise and own past data breaches, was or should have been well aware of the risk of data breaches of its own databases, and should have taken reasonable steps to prevent the data breach in the first place, or to detect the data breach sooner than it did.

---

[16] https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#6495a79c677c (dated September 8, 2017, last accessed September 21, 2017).

[17] *Id.*

Equifax – The Present Data Breach

40. On July 29, 2017, Equifax purportedly discovered that one or more unauthorized persons accessed data housed on its servers.[18]

41. On September 7, 2017, Equifax "announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers." Equifax stated that the data breach occurred as a resulted of a "website application vulnerability" that was "exploited" and permitted access, among other things, to "names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers." Furthermore, "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." [19] Equifax indicated that, "[b]ased on the company's investigation, the unauthorized access occurred from mid-May through July 2017."[20]

42. Equifax's September 7, 2017 announcement also indicated that it "has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases."[21]

43. Despite Equifax's professed expertise in the area of data protection, management and customer support, both its lapse in security which permitted the breach and its response to this breach have been inadequate.

44. Equifax did not announce that its data systems maintaining PII of its customers was compromised immediately upon learning of the breach on July 29, 2017. Instead, Equifax waited nearly 6 weeks, until September 7, 2017, to announce

---

[18] https://www.equifaxsecurity2017.com/ (last accessed September 21, 2017).

[19] *Id.*

[20] *Id.*

[21] *Id.*

that its systems were compromised, and that up to 143 million consumers' records had been taken.

45. Moreover, Equifax is still delaying notifying individual customers affected by the breach by refusing to notify all but a few hundred thousand out of the 143 million affected customers, despite having email addresses for many of them. This failure to notify violates numerous state notification statutes, including Cal. Civ. Code 1798.82(j)(3)(A).

46. According to their September 7, 2017 announcement, Equifax is only planning to "send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted."[22] This means that they will directly notify less than 0.3% of the 143 million people who are victims of this data breach, leaving everyone else to have to take actions to try to find out if they are a victim.

47. Equifax has created a website, www.equifaxsecurity2017.com, purportedly "to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection," [23] as described *supra*.

48. Equifax's website requires people to type in more personal information (i.e., last name and six digits of your social security number) to find out only if you may be affected without any further details about what of their information was taken. Understandably, many customers may well be reluctant to provide more PII electronically to Equifax given its clear failure to safeguard the PII it already has. This constitutes an unlawful and inadequate form of substitute notice.

49. Once someone figures out if they are a victim of this data breach, all Equifax has offered them to date is the opportunity to sign up for a "credit file

---

[22] *Id.*

[23] *Id.*

monitoring and identity theft protection" called TrustedID Premier, which "includes 3-Bureau credit monitoring of Equifax, Equifax and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers."[24] It is offering this protection "complimentary for one year."[25]

50. Equifax's data breach website has been confusing and made it appear that one must sign up for its monitoring product to learn if they are a victim of Equifax's data breach. Specifically, the "Schedule. Enroll. Activate." section of the equifaxsecurity2017.com website, which has since been changed, stated that

> [t]o enroll and activate your complimentary identity theft protection and credit file monitoring product, called TrustedID Premier, please follow the steps outlined below. At the beginning of this process, you will find out whether your personal information may have been impacted by this incident.[26]

51. Equifax initially required all persons signing up for TrustedID Premier to agree to an arbitration clause and class action waiver that could limit their ability to participate in a class action concerning the data breach. "Buried in the terms of service is language that appears to bar those who enroll in an Equifax credit monitoring program from participating in any class-action lawsuits that may arise from the incident."[27]

52. Subsequently, Equifax announced that it removed the language:

---

[24] *Id.*

[25] https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last accessed September 21, 2017).

[26] https://web.archive.org/web/20170907233850/https://www.equifaxsecurity2017.com/enroll/

[27] https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/what-to-know-before-you-check-equifaxs-data-breach-website/?utm_term=.69072cd46420 (updated September 10, 2017, last accessed September 21, 2017).

> Equifax issued a new statement Sunday further clarifying its stance on the arbitration clause. "To confirm, enrolling in the free credit file monitoring and identity theft protection products that we are offering as part of this cybersecurity incident does not prohibit consumers from taking legal action," Equifax said. The company said it has now removed the arbitration language from the terms of use on its data breach notification site, equifaxsecurity2017.com. It also said Sunday that the terms of use on Equifax's main site, equifax.com, do not cover the TrustedID Premier service, which has its own terms of use. "Again," Equifax continued, "to be as clear as possible, we will not apply any arbitration clause or class action waiver against consumers for claims related to the free products offered in response to the cybersecurity incident or for claims related to the cybersecurity incident itself."[28]

53. There remains skepticism regarding Equifax's use of arbitration clauses, according to Lauren Saunders, associate director of the National Consumer Law Center. "Saunders says that while Equifax backed away from its original arbitration clauses, that could change later. 'It's impossible to predict what might happen years down the road in litigation after the public spotlight fades.'"[29]

54. Additionally, many consumers may well be deterred from electronically providing Equifax with more of its PII given its inability to secure its data.

55. For any or all of these reasons, victims of the Equifax data breach may be deterred from using Equifax's website to learn if they are a victim of the data breach. Moreover, many people may have never dealt with Equifax or know what it is or know that it has any of their PII so they may not know they need to inquire to find out if they are a victim of the Equifax data breach.

56. Beyond these problems with the TrustedID Premier monitoring program offered by Equifax, providing one year of credit monitoring is woefully insufficient to redress the heightened and imminent risks of identity theft created by Equifax's Data Breach.

---

[28] *Id.*

[29] http://money.cnn.com/2017/09/15/pf/equifax-lawsuits/index.html (dated September 15, 2017, last accessed September 21, 2017).

57. Despite the fact that Equifax failed to notify the public until September 7, 2017 and offers woefully insufficient relief to its data breach victims, several Equifax executives took the opportunity to ensure their own profit by selling shares of the company valued at nearly $1.8 million just days after the Company detected the breach in late July 2017 and weeks before it made the breach public and its stock price dropped as a result.[30]

58. Equifax was aware that it needed to maintain the security of its customers' PII. In its SEC Form 10-K filings dated February 22, 2017,[31] it noted that "[w]e help consumers understand, manage and protect their personal information and make more informed financial decisions" and "[o]ur strategic objective is to be the global leader in information solutions that creates unparalleled insights to solve customer challenges. Data is at the core of our value proposition. Leveraging our extensive resources, we deliver differentiated decisions through a broad and diverse set of data assets, sophisticated analytics and proprietary decisioning technology." It further indicated that "[w]e continue to invest in and develop new technology to enhance the functionality, cost-effectiveness and security of the services we offer and further differentiate our products from those offered by our competitors." It also expressed an awareness that its "U.S. operations are subject to numerous laws and regulations governing the collection, protection and use of consumer credit and other information, and imposing sanctions for the misuse of such information or unauthorized access to data. Many of these provisions also affect our customers' use of consumer credit or other data we furnish." It indicated that "[w]e continuously monitor federal and state legislative and regulatory activities that involve credit

---

[30] https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack (dated September 7, 2017, updated September 8, 2017, last accessed September 21, 2017).

[31] Equifax's SEC Form 10-K Annual Report for the Fiscal Year Ended December 31, 2016, available at https://investor.equifax.com/financial-information/sec-filings.

reporting, data privacy and security to identify issues in order to remain in compliance with all applicable laws and regulations." As examples of these laws, it mentioned the FCRA and state laws, and noted that "[a] majority of states have adopted versions of data security breach laws that require notification of affected consumers in the event of a breach of personal information." Finally, it dedicated a whole section of the "Risk Factors" Item to the threat of security breaches, noting that it could be vulnerable to such breaches:

> ***Security breaches and other disruptions to our information technology infrastructure could interfere with our operations, and could compromise Company, customer and consumer information, exposing us to liability which could cause our business and reputation to suffer.***
>
> In the ordinary course of business, we rely upon information technology networks and systems, some of which are managed by third parties, to process, transmit and store electronic information, and to manage or support a variety of business processes and activities, including business-to-business and business-to-consumer electronic commerce and internal accounting and financial reporting systems. Additionally, we collect and store sensitive data, including intellectual property, proprietary business information and personally identifiable information of our customers, employees, consumers and suppliers, in data centers and on information technology networks. The secure and uninterrupted operation of these networks and systems, and of the processing and maintenance of this information, is critical to our business operations and strategy.
>
> Despite our substantial investment in physical and technological security measures, employee training, contractual precautions and business continuity plans, our information technology networks and infrastructure or those of our third-party vendors and other service providers could be vulnerable to damage, disruptions, shutdowns, or breaches of confidential information due to criminal conduct, denial of service or other advanced persistent attacks by hackers, employee or insider error or malfeasance, or other disruptions during the process of upgrading or replacing computer software or hardware, power outages, computer viruses, telecommunication or utility failures or natural disasters or other catastrophic events. Unauthorized access to data files or our information technology systems and applications could result in inappropriate

> use, change or disclosure of sensitive and/or personal data of our customers, employees, consumers and suppliers.
>
> We are regularly the target of attempted cyber and other security threats and must continuously monitor and develop our information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact. Insider or employee cyber and security threats are increasingly a concern for all large companies, including ours. Although we are not aware of any material breach of our data, properties, networks or systems, if one or more of such events occur, this potentially could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could subject us to litigation, regulatory fines, penalties or reputational damage, any of which could have a material effect on our cash flows, competitive position, financial condition or results of operations. Our property and business interruption insurance may not be adequate to compensate us for all losses or failures that may occur. Also, our third-party insurance coverage will vary from time to time in both type and amount depending on availability, cost and our decisions with respect to risk retention.

59. Yet, despite the previous breaches, Equifax's own promises to maintain data security, its expressed understanding of its vulnerability to data breaches, and the critical nature of maintaining the security of consumers' financial information, Equifax did not take reasonable or appropriate steps to secure the PII. As described *supra*, Equifax failed to patch the Apache Struts, despite a known vulnerability publically disclosed in early March 2017 more than 2 months before Equifax's data breach began in mid-May 2017 and almost 5 months before the Data Breach allegedly was detected on July 29, 2017 and the vulnerability allegedly patched on July 30, 2017. Furthermore, Equifax has yet to indicate that the Data was encrypted.

60. Equifax also did not disclose to anyone that it did not have adequate security systems in place to keep Plaintiff's and other customers' personal, financial

and health information that Equifax maintained on its computer systems private and secure.

61. Due to Equifax's failure to maintain the privacy and security of Plaintiff's and Class Members' private personal, financial and health information, Equifax has violated the law and breached its duties to its customers.

V. CLASS ACTION ALLEGATIONS

62. This action asserts claims on behalf of a nationwide class, and a California subclass pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), (b)(3), and (c)(4), which class and subclasses consist of persons who had their data stolen from Equifax's systems as follows:

> All persons in the United States whose personal or financial information was compromised by the data breach disclosed by Equifax on September 7, 2017 (the "National Class").
>
> All persons in California whose personal or financial information was compromised by the data breach disclosed by Equifax on September 7, 2017 (the "California Subclass").

63. Excluded from each of the class and subclasses are: (i) Equifax, Inc., its affiliated entities, and their employees, directors, principals, legal representatives, successors and assigns; and (ii) the judges to whom this action is assigned and any members of their immediate families.

64. There are thousands of members in each of the National Class and California Subclass who are geographically dispersed throughout California and the United States. Therefore, individual joinder of the members of any of the classes defined above would be impracticable.

65. Common questions of law or fact exist as to all members of the National Class and California Subclass. These common legal or factual questions include:

a. Whether Equifax engaged in the wrongful conduct alleged herein;

b. Whether Equifax's conduct was deceptive, unfair, unconscionable and/or unlawful;

c. Whether Equifax owed a duty to Plaintiff and members of the National Class and/or California Subclass to protect their PII;

d. Whether Equifax breached its duty owed to Plaintiff and members of the National Class and/or California Subclass to protect their PII;

e. Whether Equifax owed a duty to Plaintiff and members of the National Class and/or California Subclass to timely and accurately provide notice of Equifax's data breach;

f. Whether Equifax breached its duty owed to Plaintiff and members of the National Class and/or California Subclass to timely or accurately provide notice of Equifax's data breach;

g. Whether Equifax knew or should have known that its computer systems were vulnerable to attack;

h. Whether Equifax had a duty to and took reasonable and adequate steps to ensure the security of the National Class' and/or California Subclass' PII;

i. Whether Equifax breached its duty to take reasonable and adequate steps to ensure the security of the National Class' and/or California Subclass' PII;

j. Whether Equifax had a duty to encrypt Plaintiff's and members of the National Class' and/or California Subclass' PII;

k. Whether Equifax breached its duty to encrypt Plaintiff's and members of the National Class' and/or California Subclass' PII;

l. Whether Plaintiff and members of the National Class and California Subclass suffered injury as a result of Equifax's conduct or failure to act; and

m. Whether Plaintiff and members of the National Class and California Subclass are entitled to damages, restitution and/or equitable relief, including notice.

66. Plaintiff's claims are typical of the claims of the National Class and California Subclass. Plaintiff is an Equifax customer whose Personal Information was compromised by the data breach announced by Equifax on September 7, 2017. Therefore, Plaintiff is no different in any material respect from any other members of the National Class or California Subclass, and the relief sought by Plaintiff is common to the relief sought by the class and subclass.

67. Plaintiff is an adequate representative of the National Class and California Subclass because his interests do not conflict with the interests of the class or subclass members he seeks to represent, and he has retained counsel competent and experienced in conducting complex class action litigation. Plaintiff and his counsel will adequately protect the interests of the class and subclass.

68. A class action is superior to other available means for the fair and efficient adjudication of this dispute. The damages suffered by each individual member of the National Class and California Subclass are relatively small, while the burden and monetary expense needed to individually prosecute this case against Defendant is substantial. Thus, it would be virtually impossible for class and subclass members individually to redress effectively the wrongs done to them. Moreover, even if members of the class and subclass defined herein could afford individual actions, a multitude of such individual actions still would not be preferable to class wide litigation. Individual actions also present the potential for inconsistent or contradictory judgments, which would be dispositive of at least some of the issues and hence interests of the other members not party to the individual actions, would substantially impair or impede their ability to protect their interests, and would establish incompatible standards of conduct for the party opposing the class.

69. By contrast, a class action presents far fewer litigation management difficulties, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Also, or in the alternative, the National Class and California Subclass may be certified because Defendant has acted or refused to act on grounds generally applicable to each of the respective class and subclass, thereby making preliminary and final declaratory relief appropriate. Also in the alternative, the National Class and California Subclass may be certified with respect to particular issues pursuant to Fed.R.Civ.P. 23(c)(4).

70. All records concerning Equifax's data breach, including records sufficient to identify members of the National Class and California Subclass, are in the possession and control of Equifax and its agents and are available through discovery.

VI. CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION
Willful Violation of the Fair Credit Reporting Act (on Behalf of Plaintiff and the National Class against Defendant)

71. Plaintiff hereby incorporates the foregoing paragraphs of this Complaint and restates them as if they were fully written herein.

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

73. Under the FCRA, 15 U.S.C. § 1681a(f), 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 . . . .

74. Equifax is a consumer reporting agency under the FCRA because it, for monetary fees, 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.

75. 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).

76. Under the FCRA, 15 U.S.C. § 1681a(d)(1), 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.

77. The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Plaintiff and 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 Plaintiff's and Class Members' eligibility for credit.

78. 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 Plaintiff's and Class Members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

79. Equifax furnished the Plaintiff's and 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.

80. The Federal Trade Commission ("FTC") has indicated its intent to take 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.[32]

81. 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, Equifax's admitted failure to correct until July 30, 2017 a known vulnerability publically disclosed more than 2 months before the data breach began in mid-May 2017 that permitted the instant Data Breach and other data breaches in the past. Further, Equifax touts itself as an industry leader in managing and protecting data; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

82. 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 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

[32] Statement of Commissioner Brill (Federal Trade Commission 2011), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonestatement.pdf (revised August 15, 2011, last accessed September 25, 2017).

requirements, an understanding that was expressed in its 10-K cited *supra*. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiff and other Class Members of their rights under the FCRA.

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

84. Plaintiff and the Class Members have been damaged by Equifax's willful failure to comply with the FCRA. Therefore, Plaintiff and each of the 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).

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

SECOND CAUSE OF ACTION
Negligent Violation of the Fair Credit Reporting Act (on Behalf of Plaintiff and the National Class against Defendant)

86. Plaintiff hereby incorporates the foregoing paragraphs of this Complaint and restates them as if they were fully written herein.

87. 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, Equifax's admitted failure to correct until July 30, 2017 a known vulnerability publically disclosed more than 2 months before the data breach began in mid-May 2017 that permitted the instant data breach and other data breaches in the past. Further, as an enterprise claiming to be an industry leader in managing and protecting data, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

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

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

90. Plaintiff and 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).

THIRD CAUSE OF ACTION
Negligence (on Behalf of Plaintiff and the National Class against Defendant)

91. Plaintiff hereby incorporates the foregoing paragraphs of this Complaint and restates them as if they were fully written herein.

92. 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 Plaintiff's and Class Members' information was adequately secured from unauthorized access. This duty also included, at the minimum, that Plaintiff's and Class Members' PII be maintained in encrypted form.

93. Equifax's privacy policy acknowledged Equifax's duty to adequately protect Plaintiff's and Class Members' PII. Specifically, it states,

> 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.[33]

[33] http://www.equifax.com/privacy/ (last accessed September 21, 2017).

94. Equifax owed a duty to Plaintiff and National Class Members to implement intrusion detection processes that would detect a data breach in a timely manner, and to act upon any warnings or alerts that its security systems were breached.

95. Equifax owed a duty to Plaintiff and National Class Members to timely disclose any breach of its security systems.

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

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

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

99. 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.

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

101. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Plaintiff's and Class Member's PII, including Equifax's admitted failure to correct until July 30, 2017 a known vulnerability publicly disclosed more than 2 months before the data breach began in mid-May 2017 that permitted the instant data breach; (b) failing to implement processes to detect a breach of its security systems in a timely manner, and to act upon any warnings or alerts that Equifax's security systems were breached; (c)

failing to detect the Data Breach in a timely manner; and (d) failing to disclose that Defendant's data security practices were inadequate to safeguard Plaintiff's and Class Member's PII.

102. Equifax also breached its duties by failing to provide adequate and timely notice of the breach.

103. Specifically, by their own admission, Equifax discovered the breach on July 29, 2017, but did not publicly announce the breach until September 7, 2017.

104. Furthermore, despite the fact that around 143 million customers had PII that was accessed as a result of the breach, according to their September 7, 2017 announcement and the fact that Equifax has the names, addresses and emails for most or all of those customers, Equifax is only planning to "send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted."[34] This constitutes less than 3% of those affected by the breach.

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

106. 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 Plaintiff and Class Members.

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

108. 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 more closely monitor their financial accounts and

---

[34] https://www.equifaxsecurity2017.com/ (last accessed September 21, 2017).

credit histories 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 Member's PII has also diminished the value of the PII.

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

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

FOURTH CAUSE OF ACTION
Negligence Per Se (on Behalf of Plaintiff and the National Class against Defendant)

111. Plaintiff hereby incorporates the foregoing paragraphs of this Complaint and restates them as if they were fully written herein.

112. 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).

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

114. 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 Plaintiff and Class Members.

115. Equifax also failed to notify affected customers in accordance with various state laws, the applicability of which they recognized in their 10-K, as cited *supra*.

116. Defendant's failure to comply with the applicable laws and regulations constitutes negligence *per se*.

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

118. 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 more closely monitor their financial accounts and credit histories 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.

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

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

FIFTH CAUSE OF ACTION
Constructive Fraud (on Behalf of Plaintiff and the National Class against Defendant)

121. Plaintiff hereby incorporates the foregoing paragraphs of this Complaint and restates them as if they were fully written herein.

122. Equifax owed a duty to Plaintiff and Class Members to adequately protect their PII under various state and federal laws and regulations by virtue of being a consumer reporting agency.

123. As a consumer reporting agency to whom Plaintiff's and Class Members' most intimate, sensitive and private personal information and PII was provided, Equifax enjoyed a special relationship of trust and confidence with Plaintiff and Class

Members and owed them a heightened duty above and beyond normal commercial relations. Accordingly, Plaintiff and Class Members reasonably expected Equifax would adhere to its obligations to adequately protect the sensitive, personal information they provided including the PII Equifax allowed to be stolen.

124. Equifax breached this duty by failing to maintain security adequate to protect Plaintiff's and Class Members' PII, and by failing to timely and adequately notify them of the breach.

125. As a result of Equifax's conduct, Plaintiff and Class Members are entitled to damages and equitable relief.

SIXTH CAUSE OF ACTION
Violations of the California Data Breach Act, California Civil Code §§ 1798.80, *et seq*. (on Behalf of Plaintiff and the California Subclass against Defendant)

126. Plaintiff hereby incorporates the foregoing paragraphs of this Complaint and restates them as if they were fully written herein.

127. Plaintiff's and the California Subclass Members' PII which was taken in the data breach revealed by Equifax on September 7, 2017 includes protected personal information under California's Data Breach Act, California Civil Code §§ 1798.80, *et seq*.

128. "[T]o ensure that personal information about California residents is protected," Equifax was required to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect" Plaintiff's and California Subclass Members' "personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code. § 1798.81.5.

129. Under Cal. Civ. Code §1798.81, Equifax was required to

> take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means.

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

131. Under Cal Civ. Code §1798.82(a), it is therefore required to

> 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….

132. In the alternative, Equifax maintains computerized data that includes personal information that it does not own, as defined by Cal. Civ. Code § 1798.80 *et seq.* It would therefore be bound by Cal Civ. Code §1798.2(b), which 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.

133. Cal Civ. Code § 1798.82(d) sets forth specific requirements for breach disclosures; §1798.82(j) allows, under certain circumstances, the company in question to provide substitute service, including "Email notice when the person or business has an email address for the subject persons."

134. Equifax has violated California's Data Breach Act by (i) failing to implement and maintain reasonable security procedures and practices to protect Plaintiff's and California Subclass Members' personal information from unauthorized access, destruction, use, modification, or disclosure; (ii) failing to take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means; and (iii) failing to disclose in the most expedient time possible without delay that California residents' unencrypted personal information was, or was reasonably believed to have been, acquired by an unauthorized person, in the manner prescribed

by California law, including the fact that Equifax failed to provide email notice to affected individuals even when they had email addresses for such individuals.

135. Cal Civ. Code §1798.84(b) provides that "customers injured by a violation" of California's Data Breach Act "may institute a civil action to recover damages"; §1798.84(c) provides that customers injured by violations of § 798.83 are entitled to civil penalties per violation; and §1798.84(g) states that a "[a] prevailing plaintiff in any action commenced under Section 1798.83 shall also be entitled to recover his or his reasonable attorney's fees and costs."

136. Cal Civ. Code § 1798.84(e) states that a "business that violates, proposes to violate, or has violated this title may be enjoined."

137. As a result of Equifax's violation of California's Data Breach Act, Plaintiff and California Subclass Members are entitled to recover damages (including civil penalties) sustained as a result of Equifax's violation of the Data Breach Act, as well as attorneys' fees, costs, and expenses incurred in bringing this action. Plaintiff and California Subclass Members are also entitled to the requested injunctive relief, including directing Equifax to provide notice of the data breach and what data of theirs was accessed to California Subclass Members for whom Equifax has an email address.

SEVENTH CAUSE OF ACTION
Violation of California's Unfair Competition Law, Bus. & Prof. Code §§ 17200, *et seq*. (on behalf of Plaintiff and the California Subclass against Defendant)

138. Plaintiff hereby incorporates the foregoing paragraphs of this Complaint and restates them as if they were fully written herein.

139. Plaintiff brings this cause of action on behalf of himself and the members of the California Subclass.

140. Equifax violated (and continues to violate) California's Unfair Competition Law ("UCL"), California Business & Professions Code § 17200 *et seq.*, by engaging in unlawful, unfair, fraudulent, deceptive, untrue, and misleading acts and practices.

141. California Business & Professions Code § 17200 prohibits any "unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising."

142. 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 California Subclass 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 California 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 California Class Members' PII;

e. Equifax knowingly omitted, suppressed, and concealed the inadequacy of its privacy and security protections for California 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 California Class Members in a timely and accurate manner, in violation of the duties imposed by Cal. Civ. Code § 1798.82 *et seq*.

143. 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 Plaintiffs and the California Subclass.

144. A business act or practice is "unlawful" if it violates any established state or federal law.

145. Equifax's acts and practices constitute "unlawful" business acts and practices by virtue of their violation of the FCRA, 15 U.S.C. §§ 1681e (as described fully *supra*); the California Customer Records' Act, Cal. Civ. Code §§ 1798.80, *et seq.* (as described fully *supra*); Cal. Bus. & Prof. Code §§ 17200, *et seq.* (as described fully *supra*); and California common law.

146. There were reasonably available alternatives to further Equifax's legitimate business interests, including using best practices to protect California Class Members' PII, other than Equifax's wrongful conduct described herein.

147. As a direct and/or proximate result of Equifax's unlawful, unfair, and/or fraudulent practices, Plaintiff and the California Subclass have suffered injury in fact in connection with the Data Breach, including but not limited to time and/or 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 California Class Members are entitled to compensation, restitution, disgorgement, and/or other equitable relief. Cal. Bus. & Prof. Code § 17203.

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

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

150. Through their unlawful, unfair, and/or fraudulent acts and practices, Defendant has obtained, and continues to unfairly obtain, money from members of the California Subclass. Under the UCL, Plaintiff seeks restitution of money or property that the Defendant may have acquired by means of its unlawful, unfair, and/or fraudulent business practices (to be proven at trial), restitutionary disgorgement of all profits accruing to Defendant because of its unlawful, unfair, and/or fraudulent business practices (to be proven at trial), declaratory relief, and attorney's fees and costs (allowed by Cal. Code Civil Pro. §1021.5).

151. Plaintiff and other California Subclass Members also are entitled to injunctive relief, under California Business and Professions Code §§ 17203, 17204, to stop Equifax's unlawful, unfair, and/or fraudulent business practices and to require Equifax to maintain adequate security measures to protect the personal and financial information in its possession.

152. As such, Plaintiff requests on behalf of himself and all California Subclass Members the relief set forth in the Prayer, including that this Court enjoin Defendant from continuing to violate the UCL as discussed herein. Otherwise, the California Subclass may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

VII. PRAYER

WHEREFORE, Plaintiff, on behalf of himself and all members of the National Class and California Subclass, requests that the Court order the following relief and enter judgment against Equifax as follows:

A. An order certifying that this action is properly brought and may be maintained as a class action, that Plaintiff Albert Louis Fried be appointed a Class

Representatives for the National Class and California Subclass, and that Plaintiff's counsel be appointed Counsel for the National Class and California Subclass.

B. Injunctive relief requiring Defendant to (1) strengthen its data security systems that maintain PII to comply with the FCRA, California law, and any other applicable law and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendant's systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond, and (5) provide notice of the data breach specifying what data was accessed;

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

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

E. An award to Plaintiff and all Class Members (and Subclass Members) of additional credit monitoring and identity theft protection services beyond the package Equifax is currently offering;

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

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

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

IX. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims and/or issues so triable.

DATED: September 26, 2017

Respectfully Submitted,

/s/William T. Payne
William T. Payne (CSB 90988)

Joseph N. Kravec, Jr. (to be admitted *pro hac vice*)
FEINSTEIN DOYLE PAYNE & KRAVEC, LLC
Law & Finance Building, Suite 1300
429 Fourth Avenue
Pittsburgh, PA 15219-1639
Tel: (412) 281-8400
Fax: (412) 281-1007
Email: wpayne@fdpklaw.com
Email: jkravec@fdpklaw.com

ATTORNEYS FOR PLAINTIFF AND THE PROPOSED CLASS AND SUBCLASS

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

ALBERT LOUIS FRIED, on behalf of himself and all others similarly situated,

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Feinstein Doyle Payne & Kravec, LLC
429 Fourth Avenue, Law & Finance Building, Suite 1300
Pittsburgh, PA 15219 (412) 281-8400

DEFENDANTS

EQUIFAX, INC., a Georgia corporation, and DOES 1-100

County of Residence of First Listed Defendant Fulton
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

'17CV1955 CAB KSC

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. Section 133; 15 U.S.C. Section 1681e, et seq.

Brief description of cause:
Failure to Maintain Reasonable Procedures

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ in excess of $5,000,000.00

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Honorable Marilyn L. Huff DOCKET NUMBER 3:17-cv-1828

DATE 09/26/2017

SIGNATURE OF ATTORNEY OF RECORD
/s/ William T. Payne

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.

TABLE OF CONTENTS

Create an Account

Email Address

Confirm Email Address

User Name

Password

Confirm Password

Secret Question: Please select a security questio

Answer to Secret Question

Confirm Answer

Select Payment Type

We will require you to provide your payment information when you sign up and we will immediately charge your card $15.95. Product is active for 30 days once purchased. Cancellation is not applicable to one-time report products and we do not offer refunds.

Credit/Debit Card Type: VISA MasterCard AMEX DISC

Card Number | Security Code

Expiration Date: 01 / 17

Save this method of payment for future purchases.

Billing ZIP Code

Promotion Code | Apply

Terms of Use

I accept and agree to the Terms of Use, including the arbitration provisions, and acknowledge that I have received the Privacy Notice.

You understand and agree that by clicking on the Continue button, you are providing "written instructions" in accordance with the Fair Credit Reporting Act authorizing Equifax Consumer Services LLC to obtain your credit information from the personal credit report maintained by one or more of the three nationwide credit reporting agencies and you hereby authorize Equifax Consumer Services LLC to access your personal credit information in order to confirm your identity and display your credit data to you related to your use and enjoyment of the product.

Continue

You Have Selected

Equifax Credit Report and Score

Total: $ 15.95

We will require you to provide your payment information when you sign up and we will immediately charge your card $15.95. Product is active for 30 days once purchased. Cancellation is not applicable to one-time report products and we do not offer refunds.

Privacy Notice

Our Privacy Notice describes how we collect, use and share your information, and your right to limit sharing of your personal information, except as required or permitted by law. By checking the box below, you may choose to opt out of Equifax Consumer Services LLC sharing your personal information (1) for our affiliates to market to you; (2) for nonaffiliates to market to you; and (3) with respect to information about your creditworthiness, for our affiliates' everyday business purposes.

I choose to opt out.

EXHIBIT 1

Page 1

EQUIFAX

Research Request Form

You may initiate an investigation request via the internet at www.investigate.equifax.com.

Or, mail this document to the following address:

Equifax Information Services LLC
P.O. Box 740256
Atlanta, GA 30348

Email Address (please print clearly): _____

**Please provide your email address if you would like to be informed once your reinvestigation is completed and if you would like to view the results of your reinvestigation online.*

Would you like Equifax to hide the first 5 digits of your social security number on our response to you? Circle: Yes No

Confirmation Number (please provide if you have a confirmation number): _____

Intentionally making any false statements to a consumer reporting agency for the purpose of having it placed on a consumer report is punishable by law in some states. To ensure that your request is processed accurately, please enlarge photocopies of any items that contain small print (i.e. driver's license, W2 forms, etc.). Photocopies that are not legible or contain highlighting may cause us to request that you resubmit your request for clarity.

If your identity information differs from the information listed on this form, please fill in the correct information in the space provided for each item. Please provide a photocopy of your driver's license, social security card, or recent utility bill that reflects the correct information.

Identification Information

Name _____ Social Security Number _____ Date of Birth _____

Current Address _____

Previous Address(es) _____

Daytime Phone Number _____ Evening Phone Number _____

List other names which you have used in the past _____

Account Information

Company Name _____ Account Number _____

Reason for investigation: ☐ Not Mine ☐ Paid in Full ☐ Current/Previous Status Incorrect ☐ Account Closed

☐ Other (Please explain) _____

Company Name _____ Account Number _____

Reason for investigation: ☐ Not Mine ☐ Paid in Full ☐ Current/Previous Status Incorrect ☐ Account Closed

☐ Other (Please explain) _____

Company Name _____ Account Number _____

Reason for investigation: ☐ Not Mine ☐ Paid in Full ☐ Current/Previous Status Incorrect ☐ Account Closed

☐ Other (Please explain) _____