UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

ANTHONY MIRARCHI, Individually and on Behalf of All Others Similarly Situated, **Plaintiff,** **v.** **EQUIFAX, INC.,** **Defendant.**	**CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff, Anthony Mirarchi ("Plaintiff"), on behalf of himself and others similarly situated, brings this class action against Equifax, Inc. ("Equifax" or the "Company"). Plaintiff makes the following allegations, except as to allegations specifically pertaining to Plaintiff, upon information and belief based upon, *inter alia*, the investigation of counsel and review of public documents.

NATURE OF THE ACTION

1. Plaintiff brings this class action against Equifax to seek damages and obtain an injunction to halt Equifax's practice of touting its maintenance of private consumer information and failing to secure and protect its customers' Personally Identifiable Information ("PII"), which encompasses Social Security numbers, e-mail addresses, passwords, credit and debit card numbers, and mailing and billing addresses, in accordance with both industry security standards and Equifax's own security standards. Plaintiff seeks redress for himself and all persons similarly situated who purchased Equifax products to guard against identity theft and other fraudulent activity and, in doing so, directly provided PII to the Company in addition to what it accumulated independently.

2. Equifax is a "is a leading global provider of information solutions and human resources business process outsourcing services for businesses, governments and consumers." It bills itself as the "trusted steward and advocate for our customers and consumers" and that it is "continuously improving the customer and consumer experience in our consumer and commercial offerings, anticipating and executing on regulatory initiatives, while simultaneously delivering security for our services."

3. According to its 2016 Form 10-K, filed with the U.S. Securities & Exchange Commission on February 22, 2017, Equifax's "products and services are based on comprehensive databases of consumer and business information derived from numerous sources including credit, financial assets, telecommunications and utility payments, employment, income, demographic and marketing data." Equifax then combines this information together in a credit report, which is compiled for the purpose of selling it to creditors, employers, insurers, and others who may want to access the information to make decisions about extending credit, jobs, and insurance policies, and for other purposes.

4. Through its Global Consumer Solutions segment, Equifax offered products that allegedly provided "consumers information to enable them to understand and monitor their credit and monitor and help protect their identity primarily through our Equifax Complete, ID Patrol, Credit Watch and Score Watch monitoring products." These "products also offer monitoring features for consumers who are concerned about identity theft and data breaches, including credit report monitoring from all three bureaus, internet and bank account monitoring, lost wallet support, and the ability to lock and unlock the Equifax credit file."

5. In order to purchase and use one of Equifax's products, Plaintiff and members of the Class agreed to be bound by a Product Agreement and Terms of Use (the "Product

Agreement"), which authorized the Company "to obtain, monitor and compile" their (i) "credit information from one or more consumer reporting agencies;" (ii) "'non-public personal information', 'personal information', and/or 'highly restricted personal information'" as defined by statute; and (iii) "other personal information." The Product Agreement also incorporated Equifax's Privacy Policy as a term of the contract, which provided that when consumers register to use its website or services, Equifax will collect the customer's identifying information, including "(1) information you provide directly to us; (2) information we may collect automatically, such as through cookies; and (3) other information, such as information about your device, location information, information from social networking services, and information from other sources." Equifax's Privacy Policy goes as far as to say that "[w]e collect information from you when you use this Website [connected to Equifax's personal products]." In other words, Plaintiff and the Class provided even more information to Equifax compared to the amount of information Equifax routinely collected about U.S. consumers.

6. Not surprisingly, Equifax's Privacy Policy acknowledged the importance of securely maintaining its customers' personal information, and stated that it provides reasonable security controls with respect to its customers' personal information.

7. Despite its stated commitment to "protecting the security of your personal information" in its Privacy Policy, on September 7, 2017, Equifax announced an unprecedented nationwide data breach that affected an estimated 143 million Americans (the "Data Breach"), including Plaintiff and Class members who provided their PII to Equifax to gain access to its products and services. According to Equifax's press release, unauthorized parties accessed consumers' sensitive, personal information through a "website application vulnerability" on Equifax's servers. The information included names, birth dates, Social Security numbers,

addresses, driver's license numbers, 209,000 U.S. credit card numbers, and "certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers."

8. The Data Breach occurred because Equifax failed to implement adequate security measures to safeguard the PII of Plaintiff and the Class—who purchased the Company's products and services based on representations that it would— and willfully ignored known weaknesses in its data security, including prior hacks into its information systems.

9. Indeed, former Equifax Chief Executive Officer, Richard F. Smith, told a Congressional Subcommittee that months before the cyberattack occurred, on March 8, 2017, the U.S. Department of Homeland Security, Computer Emergency Readiness Team notified Equifax (and others) about the "need to patch a particular vulnerability" in the "Apache Struts" software it used in its online portal used by consumers to dispute discrepancies on their credit reports. Smith disclosed that, although Equifax requested that employees responsible for the Apache Struts installation upgrade the software, "[w]e know that the vulnerable version of Apache Struts within Equifax was not identified or patched in response to the internal March 9 notification to information technology personnel." Likewise, scans run by Equifax's information security department that were supposed to pick up such weaknesses failed to identify the Apache Struts vulnerability. Smith admitted that "[t]he company knows . . . that it was this unpatched vulnerability that allowed hackers to access personal identifying information." Thus, as Smith acknowledged, "[b]etween May 13 and July 30, there is evidence to suggest that the attacker(s) continued to access sensitive information, exploiting the same Apache Struts vulnerability" Defendant was warned about in March 2017.

10. As a result of Equifax's failure to prevent the Data Breach, Plaintiff and Class members have been exposed to fraud, identity theft, and financial harm, as detailed below, and to

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

11. Despite a stated commitment to data security in its Privacy Policy, Equifax either failed to adequately safeguard Plaintiff's and the Class's consumer information and PII, or mishandled this information by implementing inadequate security measures to defend against data breaches. Yet, Equifax indicated that Plaintiff and the Class members were required to provide their PII and other sensitive information in order for Equifax to provide them their products and services.

12. Equifax's gross-mishandling of Plaintiff's and Class members' highly confidential personal information is particularly outrageous. Plaintiff took precautions to prevent precisely this type of injury and paid substantial sums of money to Equifax to protect his identity from theft. In doing so, he paid for products offering a "greater sense of comfort" from the risks of "identity theft."[1] In exchange for that "greater sense of comfort," Plaintiff handed-over his most highly confidential information to Equifax so that it could be tracked, and any identity theft or adverse credit event reported.

[1] Equifax, Identity Theft Protection Products, https://www.equifax.com/personal/products/identity-theft-protection.

13. Plaintiff and the Class relied on Equifax's representations and purchased Equifax's services. Yet, Equifax's admitted failure to maintain security on its data systems in the face of previous unauthorized hacks and warnings from the U.S. Government and third parties, led to the Data Breach and compromised Plaintiff's and the Class's consumer information and PII.

14. Equifax's egregious conduct in failing to secure Plaintiff's and the Class's most crucial and sensitive financial information caused them financial loss and security. In so doing, Equifax has violated multiple common law doctrines and Georgia, Pennsylvania, and Federal statutes.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because sufficient diversity of citizenship exists between parties in this action, the aggregate amount in controversy exceeds $5,000,000, and there are 100 or more members of the Class.

16. This Court has personal jurisdiction over Equifax because Equifax maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Equifax intentionally availed itself of this jurisdiction by marketing and selling products and services and by accepting and processing payments for those products and services within Georgia.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Equifax's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

18. This Court's jurisdiction to hear this action is not impeded by "Binding Arbitration" and "No Class or Representative Arbitrations" clauses in the Product Agreement. As of September

12, 2017, Equifax amended the Product Agreement and explicitly waived the clauses' applicability to the Data Breach, stating "THIS AGREEMENT . . . DOES NOT APPLY TO . . . THE EQUIFAX CYBERSECURITY INCIDENT ANNOUNCED ON SEPTEMBER 7, 2017."

19. Further emphasizing Equifax's desire to waive the restrictive terms of the Product Agreement, Equifax amended the mandatory arbitration provision to inform its customers that claims arising out of the Data Breach were not subject to mandatory arbitration: "Any claim, dispute, or controversy in which You contend that [Equifax] violated the FCRA is not subject to this provision and shall not be resolved by arbitration. The term "Claim" or "Claims" also *does not apply to any claim, dispute, or controversy related . . . to the Equifax cybersecurity incident announced on September 7, 2017*[.]"[2]

THE PARTIES

20. Plaintiff Anthony Mirarchi is a citizen and resident of the state of Pennsylvania and provided his private information to Equifax when he purchased its products and services. From July 2011 through June 2012, he subscribed to Equifax's Complete Plan, paying a $16.95 monthly fee. Starting in July 2012 through the filing of this Complaint, Plaintiff subscribed to Equifax's Complete Premier Plan, paying a $19.95 monthly fee. The services of both the Complete and Complete Premier Plans require Equifax to monitor Plaintiff's credit file and provide other services that would allow him to ensure the safety and security of his identity, credit, finances, and reputation. As part of his agreement with Equifax, he entrusted Defendants with his PII. In response to Equifax's announcement of the Data Breach, Plaintiff visited the Equifax Breach Website trustedidpremier.com in September 2017 and confirmed that his sensitive PII had indeed

[2] All emphases herein are added unless stated otherwise.

been compromised. As a result, Plaintiff has expended and will continue to expend time and resources addressing the resulting risks to his identity, credit, finances, and reputation.

21. Defendant Equifax, Inc. is incorporated in the state of Georgia. Its headquarters and principal place of business are located at 1550 Peachtree Street, NW, Atlanta, GA 30309.

22. Equifax describes itself as a "global information solutions company." Equifax "organizes, assimilates and analyzes data on more than 820 million consumers" and includes "consumer and commercial credit reporting and scoring" among its business lines.

23. Upon information and belief, each and all of the acts and omissions alleged herein were performed by, or are attributable to, Equifax and/or its employees, agents, and/or third parties acting on its behalf.

SUBSTANTIVE ALLEGATIONS

24. Equifax is one of three major nationwide credit-reporting companies that track and rate the financial history of U.S. consumers. These companies are supplied with data about loans, loan payments, and credit cards, as well as information on everything from child support payments, credit limits, missed rent and utilities payments, addresses, and employer history. All this information and more factors into credit scores.

25. Equifax primarily gets its data from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies, as well as by purchasing public records.

26. As part of its purported commitment to protecting the PII of its customers and consumers alike, Defendant asserted that it "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."[3]

27. Indeed, as Senator Sherrod Brown told former CEO Smith during a Congressional hearing, "[a] gold mine for hackers should be a digital Fort Knox when it comes to security" and that consumers "should have been able to expect that a company that gathers the most private information about them would have state-of-the-art protections for that information."

28. Prior to the Data Breach, through its Global Consumer Solutions, Equifax offered products that allegedly provided "consumers information to enable them to understand and monitor their credit and monitor and help protect their identity primarily through our Equifax Complete, ID Patrol, Credit Watch and Score Watch monitoring products." These "products also offer monitoring features for consumers who are concerned about identity theft and data breaches, including credit report monitoring from all three bureaus, internet and bank account monitoring, lost wallet support, and the ability to lock and unlock the Equifax credit file." Equifax's products "are available to consumers in the United States, Canada, and the U.K. directly primarily over the internet and indirectly through relationships with business partners who distribute our products or provide these services to their employees or customers."

29. Prior to September 7, 2017, Plaintiff purchased from Equifax the Equifax Complete™ Premier Plan. Equifax's Product Agreement provided "the terms and conditions upon which you may purchase and use our products" through owned and operated Equifax or Equifax-affiliated websites.

30. Equifax's Product Agreement states that to provide its products, the Plaintiff and members of the Class must authorize Equifax "to obtain, monitor and compile" their (i) "credit

[3] http://www.equifax.com/privacy/

information from one or more consumer reporting agencies;" (ii) "'non-public personal information', 'personal information', and/or 'highly restricted personal information'" as defined by statute; and (iii) "other personal information."

31. Equifax's Product Agreement also incorporates the Company's Privacy Policy as a term of the contract, which provides that when consumers register to use its website or services, Equifax will collect the customer's identifying information. The Privacy Policy stated that this information includes "(1) information you provide directly to us; (2) information we may collect automatically, such as through cookies; and (3) other information, such as information about your device, location information, information from social networking services, and information from other sources."

32. Not surprisingly, Equifax's Privacy Policy acknowledged the importance of securely maintaining its customers' personal information. To that end, Equifax's Privacy Policy stated that it provides reasonable security controls with respect to its customers' personal information. Indeed, in its 2016 Form 10-K, Equifax billed itself as a "trusted steward and advocate for our customers and consumers" and stated that it was "continuously improving the customer and consumer experience in our consumer and commercial offerings, anticipating and executing on regulatory initiatives, while simultaneously delivering security for our services."

33. In purchasing Equifax's services, Plaintiff provided Defendant with identifying information, including but not limited to his Social Security number, credit card information, residential address, and more. Equifax also collected additional information through Plaintiff's use of Equifax's website, including log information, device identification, and location information, as well as information from third parties, including data brokers, data cooperatives, other commercial sources, and public databases.

34. Therefore, Equifax clearly understands it has a legal and contractual obligation to protect Plaintiffs' PII.

35. After Plaintiff purchased Equifax's services, Equifax committed multiple improprieties in the management of these services and continued to deceive Plaintiff and the Class.

36. Equifax's representations and omissions gave Plaintiff the impression that the Company's management of his personal and financial information was secure.

37. However, during this time, Equifax had been making these representations and omissions knowing that it was not taking reasonable steps to secure its customers' PII.

38. Indeed, Equifax was well aware of the risks of a data breach because it markets and sells "data breach solutions" to consumers and businesses. In its marketing materials, Equifax states: "***You'll feel safer with Equifax***. We're the leading provider of data breach services, serving more than 500 organizations with security breach events everyday. In addition to extensive experience, Equifax has the most comprehensive set of identity theft products and customer service coverage in the market."[4]

39. In August 2016, MSCI ESG Research ("MSCI"), a provider of research-based indexes and analytics, downgraded Defendant to "CCC"—its lowest possible rating—because of its poor data security and privacy measures. According to Insurance Business America, MSCI's fact sheet revealed that Defendant's "data and privacy policies are limited in scope and Equifax shows no evidence of data breach plans or regular audits of its information security policies and systems[.]"[5] IBA noted that "[i]n terms of privacy and data security, one of the key issues for

[4] http://www.equifax.com/help/data-breach-solutions/.

[5] http://www.insurancebusinessmag.com/us/news/cyber/why-the-equifax-hack-was-not-a-surprise-79433.aspx

service companies rated through the MSCI ESG Ratings methodology, Equifax was assigned a zero out of 10."

Equifax Suffers a Massive Data Breach in March 2017

40. Equifax failed to heed the alarms raised by MSCI and, approximately seven months later, in March 2017, it learned that it had suffered a data breach. Following a September 18, 2017 *Bloomberg* article that highlighted the March 2017 breach, Equifax acknowledged that it had experienced a data security event involving a payroll-related service. The Company indicated that the incident had been reported to customers, affected individuals, and regulators and that it had hired independent cybersecurity forensic consulting firm Mandiant to investigate the incident.

41. In his prepared testimony before the U.S. House Subcommittee on Digital Commerce and Consumer Protection, Smith stated that, on March 8, 2017, the U.S. Department of Homeland Security, Computer Emergency Readiness Team notified Equifax (and others) about the "need to patch a particular vulnerability" in the "Apache Struts" software in its online portal used by consumers to dispute discrepancies on their credit reports. Smith disclosed that, although Defendant had requested that employees responsible for the Apache Struts installation upgrade the software, "the vulnerable version of Apache Struts within Equifax was not identified or patched in response to the internal March 9 notification to information technology personnel." Likewise, scans run by Defendant's information security department that were supposed to pick up such weaknesses failed to identify the Apache Struts vulnerability. In the end, Smith admitted that "[t]he company knows . . . that it was this unpatched vulnerability that allowed hackers to access personal identifying information."

Another Cyberattack on Equifax's Vulnerable Systems Compromised the PII of over 143 Million Americans

42. In a separate attack beginning on May 13, 2017, hackers accessed sensitive information maintained by the Company. That hack continued until July 30, 2017, during which time hackers exploited the same Apache Struts vulnerability that Equifax was warned about in March 2017. Equally as damning, Smith confessed that Equifax's "security tools did not detect this illegal access" during that two-and-a-half-month period.

43. It was not until July 29, 2017, that Equifax's security department discovered suspicious network traffic with its online dispute portal. The Company's security department blocked suspicious traffic and continued to monitor network traffic, allowing it to identify additional suspicious activity on the following day. Because of this, the security department took the web application completely offline.

44. Smith indicated that he was advised about the suspicious activity on July 31, 2017, during a conversation with Equifax's Chief Information Officer. In response, on August 2, 2017, Equifax retained the cybersecurity group of a prominent law firm, again reached out to Mandiant to investigate the suspicious activity, and contacted the Federal Bureau of Investigation.

45. By August 11, 2017, Equifax's forensic investigation (aided by external firms) "had determined that, in addition to dispute documents from the online web portal, the hackers may have accessed a database table containing a large amount of consumers' PII, and potentially other data tables." According to Smith, by the following week, on August 15, 2017, he was advised that it appeared likely that consumer PII had been stolen.

46. Smith testified that, on August 17, 2017, he held a senior leadership team meeting and received a briefing on the breach investigation. The results were alarming—"the forensic investigation had determined that there were large volumes of consumer data that had been

compromised." Smith further stated that, on August 22, 2017, he notified Equifax's lead Board member, Mark Feidler, and personnel in charge of the Company's various businesses of the Data Breach. Equifax's full Board was advised of the data breach on August 24 and 25, 2017, during special telephonic Board meetings.

47. Smith stated that, by September 4, 2017, the "investigation team had created a list of approximately 143 million consumers whose personal information we believed had been stolen[.]"

48. On September 7, 2017, Equifax issued a press release revealing to the public for the first time that "a cybersecurity incident potentially impacting approximately 143 million U.S. consumers" had occurred from mid-May through July 2017 and exposed sensitive information of the affected consumers. Equifax stated in the press release that the "information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed."

49. The press release directed consumers to a dedicated website, www.equifaxsecurity2017.com, to help "determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection." Equifax's "offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian 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 - all complimentary to U.S. consumers for one year."

50. Equifax is well aware that securing the PII it gathers is central to its business. Equifax's former CEO Smith acknowledged as much in his statement about the Data Breach: "This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes. We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations."

51. While Equifax suggested that the attackers were able to break into the Company's systems by exploiting an application vulnerability to gain access to certain files, it did not at first say which application or which vulnerability was the source of the breach. Cybersecurity blogger Brian Krebs speculated: "That the intruders were able to access such a large amount of sensitive consumer data via a vulnerability in the company's Web site suggests Equifax may have fallen behind in applying security updates to its Internet-facing Web applications. . . . It's unclear why Web applications tied to so much sensitive consumer data were left unpatched, but a lack of security leadership at Equifax may have been a contributing factor. Until very recently, the company was searching for someone to fill the role of vice president of cybersecurity, which according to Equifax is akin to the role of a chief information security officer (CISO)."[6]

52. Equifax was a known and obvious target. As noted by the *New York Times*, Equifax "is a particularly tempting target for hackers. If identity thieves wanted to hit one place to grab all the data needed to do the most damage, they would go straight to one of the three major credit reporting agencies."[7]

---

[6] Brian Krebs, *Breach at Equifax May Impact 143M Americans*, KREBS ON SECURITY, (September 7, 2017), https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/

[7] Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber, *Equifax Says Cyberattack May Have Affected 143 Million Customers*, NEW YORK TIMES, (September 7, 2017).

53. Experts agree that the Data Breach has the potential to be one of the most damaging in history. John Ulzheimer, a credit expert who previously worked at FICO and Equifax, said cybercriminals have now accessed the "crown jewels of information" at Equifax.[8] Pamela Dixon, executive director of the World Privacy Forum, a nonprofit research group, said that: "This is about as bad as it gets. If you have a credit report, chances are you may be in this breach. The chances are much better than 50 percent."[9] Avivah Litan, a fraud analyst at Gartner, stated that: "On a scale of 1 to 10 in terms of risk to consumers, this is a 10."[10]

Defendant Failed to Adequately Respond to the Data Breach

54. Equifax acknowledged that it discovered the unauthorized access on July 29, 2017, but has yet to provide individual notice to Plaintiff and many other victims of the Data Breach that their PII had been stolen and precisely what types of information were stolen. As direct customers of Equifax, Plaintiff and Class members paid Equifax to alert them of any potential risks to their credit or identity. In choosing not to immediately alert Plaintiff or the Class of the breach and ensuing risks to their credit and identity, Equifax not only breached its legal, statutory, and ethical duties to Plaintiffs, but failed to deliver the services that Plaintiff and the Class directly contracted with them to provide. Moreover, during that time affected individuals could have taken precautions like placing security freezes on their credit in order to prevent or detect fraudulent activity.

---

https://www.nytimes.com/2017/09/07/business/equifaxcyberattack.html?mcubz=0 (last visited September 8, 2017).

[8] Katie Lobosco, How to find out if you're affected by the Equifax hack, *CNNMONEY*, (September 7, 2017), https://amp.cnn.com/money/2017/09/07/pf/victim-equifax-hackhow-to-find-out/index.html.

[9] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?mcubz=0.

[10] *Id.*

55. Since publicly announcing the breach, Equifax has further perpetuated its breach of duty and breach of contract by failing to provide Plaintiff with complete and accurate information about the scope of the Data Breach and the extent to which their information has been compromised.

56. For Plaintiff and the Class, Equifax's failure to immediately and fully notify them of the breach is astounding in light of Equifax's promise to provide "Privacy Monitoring and Protection[,]" and a "greater sense of comfort" from the risks of "identity theft[.]"

57. Equifax admits knowing that Plaintiff's and Class members' information was potentially compromised before publicly announcing the Data Breach, but failed to immediately alert them, as Plaintiff and members of the Class expected under their written agreements with Equifax.

58. Instead, Plaintiff and members of the Class were treated like all other consumers, first learning their PII was comprised via Equifax's public announcement. In other words, despite agreeing to protect Plaintiff's and Class members' PII and alert them of risks of identity theft, Equifax provided them—paying customers of Equifax's identity theft protection services—no greater benefit than any other, non-paying consumer

59. Equifax's failure to alert Plaintiff and Class members that their PII was compromised before the rest of the non-customer consumers, proves that the services they paid Equifax to provide were essentially meaningless and valueless.

60. Notwithstanding the valueless nature of Equifax's services, Equifax continues to charge Plaintiff and members of the Class for their identity theft protection products.

61. Equifax's response to the Data Breach has been entirely unacceptable. While exposing Plaintiff and Class members to identity theft, a problem that will plague them for the

remainder of their lives, Equifax flouts its obligation to mitigate the damage caused by offering Plaintiff and members of the Class "complimentary"—but unsatisfactory—services for one year.

62. More absurdly, this offer is of no assistance to Plaintiff, who was already paying Equifax for the same services (and more).

63. In light of the fact that Plaintiff's and Class members' trust in Equifax to provide identity theft protection services is the reason they are now victims of identity theft, offering Plaintiff and Class members continued service with a less-comprehensive product as a remedy is is evidence of Equifax's bad faith response to this unprecedented breach.

64. As discussed above, in its press release, Equifax also directed consumers to a website it created regarding the breach, https://www.equifaxsecurity2017.com. The website purported to allow consumers to look up whether they were affected by the breach by inputting their last name and the last-6 numbers of their Social Security number, and allowed them to enroll in one year of TrustedID Premier, a credit monitoring service that is owned and operated by Equifax.

65. Compounding the insufficiency of the notice, Equifax was bizarrely unprepared to handle the traffic its website and phone lines would receive after announcing the breach of more than 143,000,000 people's PII. Equifax's website and phone lines crashed repeatedly, leaving panicked consumers unable to determine whether their information was compromised. Additionally, those consumers who did manage to get through to check whether they were affected were left confused when an apparent bug in the website coding gave them different results as to whether their information was compromised based on what browser they used. This lack of preparation for such an immensely foreseeable demand is inexplicable, and inexcusable, for an organization that holds itself out as an elite information technology company.

66. Almost immediately after its announcement, Equifax's websites started malfunctioning. As summarized by Krebs, "the Trustedid.com site Equifax is promoting for free credit monitoring services was only intermittently available, likely because of the high volume of traffic following today's announcement. As many readers here have shared in the comments already, the site Equifax has available for people to see whether they were impacted by the breach may not actually tell you whether you were affected. When I entered the last six digits of my SSN and my last name, the site threw a 'system unavailable' page, asking me to try again later."[11]

67. Equifax executives sold at least $1.8 million worth of shares after the Company discovered suspicious activity, but well before the public disclosure of the Data Breach. Equifax's Chief Financial Officer, John Gamble, sold shares worth $946,374; Equifax's president of U.S. information solutions, Joseph Loughran, exercised options to dispose of stock worth $584,099; and Equifax's president of workforce solutions, Rodolfo Ploder, sold $250,458 of stock. The U.S. Department of Justice is conducting an investigation into these sales.

What the Data Breach Means for Plaintiff and the Class

68. As a result of Equifax's negligent security practices and delay in notifying affected individuals, Plaintiff and other Class members are at imminent risk of identity theft and now face years of constant monitoring of their financial and personal accounts and records to guard against identity theft and fraud. Plaintiff and Class members may be faced with fraudulent debt, or incur costs for, among other things, paying monthly or annual fees for identity theft and credit monitoring services, obtaining credit reports, credit freezes, and other protective measures to deter, detect, and mitigate the risk of identity theft and fraud.

[11] Brian Krebs, Breach at Equifax May Impact 143M Americans, Krebs On Security, (September 7, 2017), https://krebsonsecurity.com/2017/09/breach-at-equifax-mayimpact-143m-americans/.

69. The U.S. Social Security Administration (the "SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[12] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought." In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[13]

70. The information Equifax allowed "criminals" to access can and likely will be employed to effect massive identity theft, invade bank accounts, make unauthorized purchases, and commit various crimes in the names of the unsuspecting victims.

71. The breach is particularly egregious because the vast majority of information Equifax allowed unauthorized third-parties to access was obtained without the knowledge or consent of consumers, often reported by lending institutions and other third-party entities.

72. For Plaintiff and the Class, the breach is even more disturbing, because they paid Equifax to protect the very information that was compromised.

73. Plaintiff has been a customer since January 2011 and, as such, has paid Equifax nearly $240 each year for its Complete Premier Plan. Plaintiff expected Equifax to monitor his credit, alert him to any unauthorized and suspicious activity, and insure him against identity theft and data breaches resulting in losses to Plaintiff. Equifax agreed to provide those services.

---

[12] *Identity Theft And Your Social Security Number, Social Security Administration* (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

[13] *Id.*

74. As discussed above, to use its products, Equifax required Plaintiff to provide his most sensitive personal identifiers, along with a nominal annual fee, in exchange for a "greater sense of comfort" from the risks of "identity theft."

75. Plaintiff fully expected Equifax to safeguard his information with the highest level of security, relying on Equifax's representations in its Privacy Policy that it is "committed to protecting the security of [customers'] personal information" through the "use [of] technical, administrative and physical security measures that comply with applicable federal and state laws[,]" and that Equifax "pride[s] [itself] on being a leader in managing and protecting data[.]" Absent these guarantees, Plaintiff would never have provided Equifax with his PII.

76. As a direct and proximate result of Equifax's actions and omissions, Plaintiff and the Class have suffered and will continue to suffer harm, injury, and damage. The unauthorized disclosure and use of their PII has caused injuries contemplated by our congressional leaders, and which they sought to prevent by enacting the Fair Credit Reporting Act ("FCRA") and the Graham-Leach-Biley Act ("GLBA").

77. Plaintiff and the Class also suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property that Plaintiff and Class members entrusted to Equifax and that was compromised in and as a result of the Data Breach.

78. Plaintiff and the Class also suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their PII being placed in the hands of unauthorized users who have already, or will imminently, misuse such information.

79. Moreover, Plaintiff and the Class have a continuing interest in ensuring that their PII, which remains in the possession of Equifax, is protected and safeguarded from future breaches.

80. At all relevant times, Equifax was well-aware, or reasonably should have been aware, that the PII collected, maintained and stored in its systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

81. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of unauthorized users. Despite the frequent public announcements of data breaches of corporate entities, including Experian (one of Equifax's two major competitors), Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiff and the Class.

82. PII is a valuable commodity to criminals. A "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground Internet websites. PII is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards. Moreover, identity thieves may commit various types of government fraud such as immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

83. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

84. Equifax was, or should have been, fully aware of the significant number of people whose PII it collected, and thus, the significant number of individuals who would be harmed by a breach of Equifax's systems.

85. Despite all of the publicly available knowledge of the continued compromises of PII in the hands of other third parties, Equifax's approach to maintaining the privacy and security of the PII of Plaintiff and Class members was, at the very least, negligent.

86. The ramifications of Equifax's failure to keep Plaintiff's and Class members' data secure are severe.

87. Equifax is prohibited by the Federal Trade Commission Act (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has found that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act.[14]

88. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 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."

89. Equifax is required by state and federal laws and regulations to protect individuals' PII.

90. In addition to its obligations under federal and state laws, Equifax owed a duty to Plaintiff and Class members, who entrusted it with sensitive personal information based on Equifax's representations in its Product Agreements and Privacy Policy, to exercise reasonable

[14] *See e.g.*, *FTC v. Wundham Corp.*, 799 F.3d 236, 243 (3d Cir. 2015).

care in obtaining, retaining, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Equifax owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PII of Plaintiff and Class members.

91. Equifax owed a duty to Plaintiff and Class members to design, maintain, and test its computer systems to ensure that the PII in its possession was adequately secured and protected because they directly and indirectly provided PII to Equifax when they each purchased Equifax products and services based on the Company's representations about privacy and security in, among other places, its Product Agreements and Privacy Policy.

92. Equifax owed a duty to Plaintiff and Class members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including adequately training its employees and others who accessed PII within its computer systems on how to adequately protect PII because they directly and indirectly provided PII to Equifax when they each purchased Equifax products and services based on the Company's representations about privacy and security in, among other places, its Product Agreements and Privacy Policy.

93. Equifax owed a duty to Plaintiff and Class members to implement processes that would deter a breach of its data security systems because they directly and indirectly provided PII to Equifax when they each purchased Equifax products and services based on the Company's representations about privacy and security in, among other places, its Product Agreements and Privacy Policy.

94. Equifax owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate and insufficient data security practices.

Equifax collected Plaintiff and Class members' information directly when they purchased Equifax products as well as indirectly from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies, as well as by purchasing public records.

95. The Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

96. Equifax had the resources to prevent a breach, but neglected to adequately invest in data security, despite being directly warned about certain vulnerabilities by the U.S. Department of Homeland Security and the growing number of well-publicized data breaches, including one it sustained in March 2017.

97. Had Equifax remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Equifax would have prevented the Data Breach and, ultimately, the theft of Plaintiff's and Class members' PII.

98. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including but not limited to:

a. Theft of their personal and financial information;

b. Unauthorized charges on their debit and credit card accounts;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of unauthorized users and already misused via the sale of Plaintiffs' and Class members' information on the black market;

d. The untimely and inadequate notification of the Data Breach;

e. The improper disclosure of Plaintiffs' and Class members' PII;

f. Loss of privacy;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

i. Ascertainable losses in the form of the loss of cash back or other benefits as a result of inability to use certain accounts and credit cards affected by the Data Breach;

j. Loss of use and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and

k. The loss of productivity and value of their time spent to attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, canceling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

99. Reimbursing Plaintiff and the Class solely for the financial losses suffered due to Equifax's failure to discharge its obligations established for each of the products and services they paid for does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft

victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.

100. Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency's slippage, as is the case here.

101. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [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.

102. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

103. The PII of Plaintiff and Class members is private and sensitive in nature and was left inadequately and insufficiently protected by Equifax. Equifax did not obtain Plaintiff's and Class members' consent to disclose their PII to any other person as required by applicable law and industry standards. Equifax has not offered customers any meaningful credit monitoring or identity theft protection services, despite the fact that it is well known and publicly acknowledged that damage and fraud from a data breach can take years to occur. As a result, Plaintiff and Class members are left to their own actions to protect themselves from the financial damage Equifax has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Equifax's actions have created for Plaintiff and Class members, is ascertainable and is a determination appropriate for the trier of fact. Equifax has also not offered to cover any of the damages sustained by Plaintiff or Class members.

104. While the PII of Plaintiff and members of the Class has been stolen, Equifax continues to hold PII of consumers, including Plaintiff and Class members. Particularly because Equifax and has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and members of the Class have an undeniable interest in insuring that their PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ACTION ALLEGATIONS

105. Plaintiff brings this action, on behalf of himself and all others similarly situated, and thus, seeks class certification under Federal Rules of Civil Procedure. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and (c)(4), Plaintiffs seeks certification of a nationwide class defined as follows:

> All persons in the United States who entered into an agreement for services or products with, or who otherwise directly transmitted to Defendants, any of their

> PII, and whose PII was compromised as a result of the Data Breach announced by Equifax in September 2017.

106. Pursuant to Fed. R. Civ. P. 23, and in addition to claims asserted on behalf of the Class, Plaintiff asserts claims under the laws of the individual States in which he respectively resides, and on behalf of separate statewide classes, defined as follows:

> All persons residing in [STATE] who entered into an agreement for services or products with, or who otherwise directly transmitted to Equifax, any of their PII, and whose PII was compromised as a result of the Data Breach announced by Equifax in September 2017 (the "Statewide Classes").

107. Excluded from each of the above Classes are Equifax and any of its affiliates, parents or subsidiaries; all employees of Equifax; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

108. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

109. *Numerosity and Ascertainability*: The members of the Classes are so numerous and geographically dispersed that individual joinder of all class members is impracticable. While Plaintiff is informed and believes that there are millions of class members, the precise number of class members is unknown to Plaintiff, but will be determined through discovery. Class members' names and addresses are ascertainable and identifiable through information in Equifax's records, and Class members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

110. *Commonality*: This action involves several critical common questions of law and fact, which predominate over any questions affecting individual class members, including, without limitation:

a. Whether Equifax had a duty to protect PII;

b. Whether Equifax knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether Equifax's security measures to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Equifax was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Equifax's failure to implement adequate data security measures allowed the breach to occur;

f. Whether Equifax's conduct constituted deceptive trade practices;

g. Whether Equifax's conduct, including their failure to act, resulted in or was the proximate cause of the breach of it systems, resulting in the loss of the PII of Plaintiff and Class members;

h. Whether Plaintiff and Class members were injured and suffered damages or other acceptable losses because of Equifax's failure to reasonably protect it systems and data networks;

i. Whether Plaintiff and Class members were injured and suffered damages or other acceptable losses because of Equifax's failure to reasonably inform Plaintiff and Class members of the data breach;

j. Whether Equifax breached its contractual obligations to Plaintiff and the Class to monitor their credit and identify and provide "alerts" of suspicious activity as promised;

k. Whether Equifax breached its contractual duty of good faith and fair dealing by failing to timely notify Plaintiff and Class members of the breach; and

l. Whether Plaintiff and Class members are entitled to relief.

111. *Typicality*: Plaintiff's claims are typical of the Class members' claims because Plaintiff and other Class members purchased products from Equifax and all had their PII

compromised in the Data Breach. Furthermore, the factual basis of Equifax's conduct are common to all Class members and represents a common thread of deliberate, negligent, and/or fraudulent misconduct resulting in injury to all Class members.

112. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the Classes he seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting statewide, multistate and national consumer class actions. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the classes they represent, and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to the class.

113. *Superiority*: Plaintiff and Class members have suffered and will continue to suffer harm and damages as a result of Equifax's conduct. A class action is superior to all other available methods for the fair and efficient adjudication of the controversy. Absent a class action, the vast majority of Class members likely would find the cost of litigating their claims to be prohibitive, and would have no effective remedy at law. Because of the relatively small size of the individual Class members' claims, it is likely that only a few Class members could afford to seek legal redress for Equifax's conduct. Further, the cost of litigation could well equal or exceed any recovery. Absent a class action, Class members will continue to incur damages without remedy. Class treatment of common questions of law and fact would also be superior to multiple individual actions or piecemeal litigation, and that class treatment would conserve the resources of the courts and the litigants, and will promote consistency and efficiency of adjudication.

114. *Declaratory & Injunctive Relief*: Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c)(4). The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Equifax. Such individual

actions would create a risk of adjudications which would be dispositive of the interests of other Class members and impair their interests. Equifax has acted or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

115. Likewise, particular issues under Rule 23(c)(4) of the Federal Rules of Civil Procedure are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Equifax failed to timely notify Plaintiff, Class members, and/or the general public of the data breach;

b. Whether Equifax owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Equifax's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

d. Whether Equifax failed to adequately comply with industry standards amounting to negligence;

e. Whether Equifax failed to take commercially reasonable steps to safeguard the PII of Plaintiff and Class members; and

f. Whether adherence the data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

COUNT I
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

116. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

117. Plaintiff and the Class Members gave Equifax personal and sensitive information that was managed by Equifax. In exchange, Equifax was required to properly and competently manage that information with the financial and security interests of Plaintiff and the Class Members in mind. In Equifax's obligation to manage Plaintiff and the Class Members' information Equifax was obligated to act as Plaintiff and the Class Members' fiduciary.

118. Equifax, purposefully, willing, and fraudulently mismanaged the services provided to Plaintiff and the Class by providing poor security of the information. Equifax did this to extract information from the individuals and in order to increase its business venture. In so doing, Equifax solely acted in its own interests and against the interests of Plaintiff and Class Members.

COUNT II
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

119. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

120. Upon accepting and storing the PII of Plaintiff and Class members in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Equifax knew, or should have known, that the PII was private and confidential and should be protected as private and confidential.

121. Equifax owed a duty of care not to subject Plaintiff and Class members, along with their PII, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

122. Equifax knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including the breach at one of its competitors, Experian.

123. Equifax knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class members' PII.

124. Because Equifax knew that a breach of its systems would damage millions of individuals, including Plaintiff and Class members, Equifax had a duty to adequately protect their data systems and the PII contained thereon.

125. Equifax also had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, only Equifax had the ability to protect its systems and the PII it stored on them from attack. This special relationship additionally gave rise to Equifax's duty to protect Plaintiff's and the Class's PII and promptly notify them about the Data Breach.

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

127. Equifax owed numerous duties to Plaintiff and to members of the Nationwide Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices;

c. to implement processes to quickly detect the data breach and to timely act on warnings about data breaches; and

d. to warn and inform Plaintiff and Class members about the data breach in a timely fashion.

128. Despite the obvious risks to Plaintiff and the Class, Equifax breached its duties in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiff and Class members;

b. by failing to conduct regular audits of its security systems and protocols;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff and Class members PII after learning of the Data Breach;

d. by failing to comply with the minimum industry data security standards during the period of the data breaches; and

e. by failing to timely and accurately disclose that Plaintiff's and Class members' PII had been improperly acquired or accessed.

129. The law further imposes an affirmative duty on Equifax to timely disclose the unauthorized access and theft of the PII to Plaintiff and the Class so that Plaintiff and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

130. Equifax breached its duty to notify Plaintiff and Class members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiff and Class members and then by failing to provide Plaintiff and Class members information regarding the breach until September 2017. Instead, its executives disposed of at least $1.8 million worth of shares in the company after Equifax learned of the Data Breach but before it was publicly announced. To date, Equifax has not provided sufficient information to Plaintiff and Class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class.

131. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Equifax prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

132. Equifax's conduct was negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiff and Class members; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive PII had been compromised.

133. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint, nor consented to the dissemination of their PII.

134. As a direct and proximate cause of Equifax's conduct, Plaintiff and the Class suffered damages including, but not limited to: damages resulting from their purchase of products and services from Equifax; damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Class

members; damages arising from Plaintiff's and Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT III
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

135. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

136. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

137. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained

and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiff and Class members.

138. Equifax's violation of Section 5 of the FTC Act constitutes negligence per se.

139. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

140. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

141. As a direct and proximate result of Equifax's negligence per se, Plaintiff and the Class have suffered, and continue to suffer, injuries damages arising from Plaintiff's and Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT IV
BREACH OF CONTRACT
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

142. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

143. Equifax required that Plaintiff and members of the Class affirmatively assent to Equifax's Product Agreement and Terms of Use and Privacy Policy which included representations regarding Equifax's security protocols, in order to purchase the Company's services. Plaintiff relied upon Equifax's Privacy Policy and its representations regarding its practices regarding privacy and data security before purchasing Equifax's products and/or services.

144. Plaintiff and each Class member assented to Equifax policies when they purchased Equifax's products and/or services.

145. Equifax imposed upon itself an obligation to use reasonable and industry-standard security practices to protect Plaintiff's and Class members' PII.

146. Plaintiff and the Class expected that Equifax employed industry-leading security practices in accordance with its representations when making her decision to purchase Equifax's products and/or services.

147. Plaintiff and the Class performed their obligations under the agreement/s entered into with Equifax by paying the required fees and assenting to the terms and conditions of Equifax's policies.

148. By ignoring specific warnings about its vulnerabilities and implementing inferior security measures for the protection of its customers' PII, Equifax breached the terms of its contract with Plaintiff and other members of the Class to protect their PII.

149. Equifax represented to Plaintiff and the Class that they would receive, at minimum, industry-standard protection for their PII as part of Equifax's products and/or services, and that those security protections were valuable to both Plaintiff and members of the Class.

150. As a direct and proximate result of Equifax's failure to provide its customers with the level of security and protection it promised, Plaintiff and Class members have suffered injury in fact as a result of the breach.

COUNT V
BREACH OF COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

151. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

152. The law of contracts implies a covenant of good faith and fair dealing in every contract.

153. Plaintiff and the Class members contracted with Equifax by accepting Equifax's offers and paying Equifax's products and/or services.

154. Plaintiff and the Class performed all or substantially all of their duties under their agreement/s with Equifax.

155. The conditions required for Equifax's performance under the contracts has occurred.

156. Equifax failed to provide and/or unfairly interfered with and/or frustrated the right of Plaintiff and members of the Class to receive the full benefits under their purchase agreements.

157. Equifax breached the covenant of good faith and fair dealing implied in its contracts with Plaintiff and the Class members by, among other things, failing to use and provide reasonable

and industry-leading security practices, an aspect of the parties' course of dealing by which Equifax exercised unilateral discretion and control.

COUNT VI
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

158. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

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

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

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

162. 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).

163. Under the FCRA, a "consumer report" is defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the

purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

164. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the Nationwide Class members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

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

166. Equifax willfully and/or recklessly 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 and reckless nature of Equifax's violations is supported by, among other

things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

167. Equifax also acted willfully and recklessly 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 requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiff and other members of the classes of their rights under the FCRA.

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

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

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

COUNT VII
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

171. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

172. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

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

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

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

COUNT VIII
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

176. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

177. Plaintiff and Class members entered into a contract that required Equifax to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Equifax owes duties of care to Plaintiff and Class members that require it to adequately secure PII. Equifax still possesses PII pertaining to Plaintiff and Class members.

178. Equifax has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

179. Accordingly, Equifax has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Equifax's lax approach towards data security has become public, the PII in its possession is more vulnerable than before.

180. Actual harm has arisen in the wake of the Data Breach regarding Equifax's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

181. Plaintiff, therefore, seeks a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to:

a. engaging 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, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access control so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax's systems;

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services of;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting 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 of; and

h. educating its customers and the general public 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 and the general public must take to protect themselves.

COUNT IX
VIOLATION OF THE GEORGIA FAIR BUSINESS PRACTICES ACT (O.C.G.A. § 10-1-390, *et seq.*)
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

182. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

183. Equifax, while operating in Georgia, engaged in unfair and deceptive consumer acts in the conduct of trade and commerce, in violation of O.C.G.A. § 10-1-390(a), and (b). This includes but is not limited the following:

a. Equifax failed to enact adequate privacy and security measures to protect Plaintiff's and the Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Equifax failed to take proper action 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 that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's the Class members' PII from unauthorized disclosure, release, data breaches, and theft;

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

e. Equifax knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and the Class members' PII, including but not limited to duties imposed by the FCRA, 15. U.S.C.§ 1681e, the GLBA, 15 U.S.C. § 6801 *et seq.*, and the FTC Act;

f. Equifax failed to maintain the privacy and security of Plaintiff's and the Class members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, which was a direct and proximate cause of the Data Breach; and

g. Equifax failed to disclose the Data Breach to Plaintiff and the Class members in a timely and accurate manner, in violation of § Ga. Code Ann 10-1-912.

184. As a direct and proximate result of Equifax's violation of the Georgia Fair Business Practices Act, Plaintiff and the Class suffered damages including, but not limited to: damages arising from unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of their PII; damages arising from Plaintiff's inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to, late fees, charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, among other things, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

185. Equifax's actions and conduct in violating the Georgia Fair Business Practices Act have caused, or are likely to cause, substantial damage to Plaintiff and the Class that includes:

a. Fraudulent charges on their debt and credit card accounts which may not be reimbursed;

b. Theft of their PII by criminals;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with the fraudulent use of their financial accounts;

e. Loss of use of an access to some or all of their account funds and costs incurred as a result of being unable to access those funds;

f. Costs and list time associated with the handling and administrative consequences of the Equifax data breach, including identifying disputing and seeking reimbursement for fraudulent charges, cancelling and activating payment cards, and shopping for credit monitoring and identity theft protection; and

g. Impairment of their credit scores and ability to borrow and/or obtain credit; and

h. The continued risk of their PII which remains on Equifax's insufficiently secured systems.

186. As a result of Equifax's deceptive conduct, Plaintiff and the Class are entitled to relief, including restitution of the costs associated with the Data Breach, disgorgement of all profits accruing to Equifax because of its deceptive acts and practices, attorneys' fees and costs, declaratory relief and a permanent injunction enjoining Equifax from its deceptive trade practices.

187. Also as a direct result of Equifax's knowing violation of the Georgia Fair Business Practices Act, Plaintiff and the Class are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Equifax 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, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Equifax segment PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. Ordering that Equifax purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Equifax conduct regular database scanning and securing checks;

g. Ordering that Equifax routinely and continually 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

h. Ordering Equifax to meaningfully educate its customers and consumers about 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.

188. Plaintiff brings this action on behalf of himself and members of the Class for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow its customers and consumers to make informed purchasing decisions and to protect Plaintiff and the Class from Equifax's unfair methods of competition and unfair, deceptive fraudulent, unconscionable and unlawful practices. Equifax's wrongful conduct as alleged in this Complaint has had widespread impact on the its customers and the public at large.

189. Accordingly, Plaintiff and the Class also seek damages, equitable relief, and reasonable attorneys' fees and costs.

COUNT X
VIOLATION OF THE GEORGIA SECURITY BREACH NOTIFICATION ACT (O.C.G.A. § 10-1-912, *et seq.*)
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

190. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

191. Under O.C.G.A. § 10-1-912(a), "[a]ny information broker…that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay[.]"

192. Under O.C.G.A. § 10-1-912(b), "[a]ny person or business that maintains computerized data on behalf of an information broker … that includes personal information of individuals that the person or business does not own shall notify the information broker … of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

193. Equifax is an information broker that owns or licenses computerized data that includes personal information, as defined by O.C.G.A. § 10-1-911.

194. In the alternative, Equifax maintains computerized data on behalf of an information broker that includes personal information that Equifax does not own, as defined by O.C.G.A. § 10-1-911.

195. Plaintiff's and the Class members' PII (including but not limited to names, addresses, and Social Security numbers) includes personal information covered under O.C.G.A. § 10-1-911(6).

196. Because Equifax was aware of a breach of its security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Class members' Personal Information), Equifax had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by O.C.G.A. § 10-1-912(a).

197. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated O.C.G.A. § 10-1-912(a).

198. As a direct and proximate result of Equifax's violations of O.C.G.A. § 10-1-912(a), Plaintiff and the Class members suffered the damages alleged herein.

199. Plaintiff and the Class members seek relief under O.C.G.A. § 10-1-912 including, but not limited to, actual damages and injunctive relief.

COUNT XI
VIOLATION OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 P.S. § 201-1, *et seq.*
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

200. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

201. Plaintiff and member of the Class are "persons" within the meaning of 73 P.S. § 201-2(2).

202. Equifax is engaged in "trade" or "commerce" within the meaning of 73 P.S. § 201-2(3).

203. The Pennsylvania Unfair Trade Practices Act ("PA UTPCPL") prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce. . . ." 73 P.S. § 201-3.

204. As alleged throughout this Complaint, Equifax's deliberate conduct constitutes deceptive acts or practices in the conduct of business trade or commerce and furnishing of services including:

a. Equifax failed to enact adequate privacy and security measures to protect Plaintiff's and the Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Equifax failed to take proper action 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 that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's the Class members' PII from unauthorized disclosure, release, data breaches, and theft;

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

e. Equifax knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and the Class members' PII, including but not limited to duties imposed by the FCRA, 15. U.S.C.§ 1681e, the GLBA, 15 U.S.C. § 6801 *et seq.*, and the FTC Act;

f. Equifax failed to maintain the privacy and security of Plaintiff's and the Class members' PII, in violation of duties imposed by applicable federal and state laws, including

but not limited to those mentioned in the aforementioned paragraph, which was a direct and proximate cause of the Data Breach; and

g. Equifax failed to disclose the Data Breach to Plaintiff and the Class members in a timely and accurate manner, in violation of 73 P.S. § 2301, *et seq.*

205. Plaintiff and the Class relied upon Equifax's deceptive and unlawful conduct.

206. Plaintiff and the Class entrusted Equifax with their PII.

207. Furthermore, as alleged above, Equifax's failure to secure consumers' PII violates the FTCA and violates the PA UTPCPL.

208. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiffs and the Class, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

209. As a direct and proximate result of Equifax's violation of the PA UTPCPL, Plaintiff and the Class suffered damages including, but not limited to: damages arising from unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of their PII; damages arising from Plaintiff's inability to use their debit or credit cards or accounts because those cards or accounts were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to, late fees, charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, among other things, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given

the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

210. Equifax's actions and conduct in violating 73 P.S. § 201-1, *et seq*. have caused, or are likely to cause, substantial damage to Plaintiff and the Class that includes:

a. Fraudulent charges on their debt and credit card accounts which may not be reimbursed;

b. Theft of their PII by criminals;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with the fraudulent use of their financial accounts;

e. Loss of use of an access to some or all of their account funds and costs incurred as a result of being unable to access those funds;

f. Costs and list time associated with the handling and administrative consequences of the Equifax data breach, including identifying disputing and seeking reimbursement for fraudulent charges, cancelling and activating payment cards, and shopping for credit monitoring and identity theft protection; and

g. Impairment of their credit scores and ability to borrow and/or obtain credit; and

h. The continued risk of their PII which remains on Equifax's insufficiently secured systems.

211. As a result of Equifax's deceptive conduct, Plaintiff and the Class are entitled to relief, including restitution of the costs associated with the Data Breach, disgorgement of all profits

accruing to Equifax because of its deceptive acts and practices, attorneys' fees and costs, declaratory relief and a permanent injunction enjoining Equifax from its deceptive trade practices.

212. Also as a direct result of Equifax's knowing violation of 73 P.S. § 201-1, *et seq.*, Plaintiff and the Class are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Equifax 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, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Equifax segment PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. Ordering that Equifax purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Equifax conduct regular database scanning and securing checks;

g. Ordering that Equifax routinely and continually 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

h. Ordering Equifax to meaningfully educate its customers and consumers about 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.

213. Plaintiff brings this action on behalf of himself and members of the Class for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow its customers and consumers to make informed purchasing decisions and to protect Plaintiff and the Class from Equifax's unfair methods of competition and unfair, deceptive fraudulent, unconscionable and unlawful practices. Equifax's wrongful conduct as alleged in this Complaint has had widespread impact on the its customers and the public at large.

214. Accordingly, Plaintiff and the Class also seek damages, equitable relief, and reasonable attorneys' fees and costs.

COUNT XII
VIOLATION OF THE PENNSYLVANIA DATA BREACH ACT (73 P.S. § 2301, *et seq.*)
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

215. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

216. By failing to timely notify Plaintiff and the Class of the Data Breach, Equifax violated Chapter 43, Section 2303 of Pennsylvania's Breach of Personal Information Notification Act, which provides, in part:

> (a) General rule.--An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4[FN1] or in order to take any measures necessary to determine the scope of the breach and to restore the

> reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.
>
> (b) Encrypted information.--An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

217. The Data Breach constituted a "Breach of the security of the system" of Equifax within the meaning of the above Pennsylvania data breach statute and the data breached was protected and covered by the data breach statute.

218. Equifax unreasonably delayed informing the public, including Plaintiff and the members of the Class, about the Data Breach after Equifax knew or should have known that the Data Breach had occurred.

219. Equifax failed to disclose the Data Breach to Plaintiff and the other members of the Class without unreasonable delay and in the most expedient time possible.

220. Equifax has provided no indication that any law enforcement agency requested that Equifax delay notification. Plaintiff and the other members of the Class suffered harm directly resulting from Equifax's failure to provide and the delay in providing notification of the Data Breach with timely and accurate notice as required by law.

221. As a result of said practices, Equifax has directly, foreseeably, and proximately caused damages to Plaintiff and the other members of the Class. Had Equifax provided timely and accurate notice of the Data Breach, Plaintiff and the other members of the Class would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Equifax in providing notice. Plaintiff and the Class could have avoided providing further data to Equifax, could have avoided use of Equifax's services, and could

otherwise have tried to avoid the harm caused by Equifax's delay in providing timely and accurate notice.

COUNT XIII
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class, or, alternatively, the Separate Statewide Classes)

222. Plaintiff incorporates by reference the previous paragraphs of this Complaint as if fully set forth herein.

223. As a result of their wrongful and fraudulent acts, concealments, and omissions pertaining to the defective state of their data security protections, as set forth above, Equifax charged a higher price for their credit monitoring and identity theft protection services than the services' true value. Equifax was also able to sell services to customers that they would have otherwise been unable to sell if customers knew their PII would not be securely stored.

224. Equifax enjoyed the benefit of increased financial gains, to the detriment of Plaintiff and other Class members, who paid a premium price that did not reflect the true value of the services offered. It would be inequitable, unjust, and unconscionable for Equifax to retain those wrongfully obtained funds.

225. Plaintiff and other Class members have no adequate remedy at law.

226. Plaintiff and other Class members therefore seek disgorgement of all profits, plus interest.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Equifax as follows:

a. For an Order certifying the classes, as defined herein, and appointing Plaintiff and their counsel to represent the Nationwide class, or in the alternative to separate Statewide Classes;

b. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

c. For equitable relief compelling Equifax to use appropriate cybersecurity methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of PII compromise;

d. For an award of damages, as allowed by law in an amount to be determined;

e. For an award of attorney's fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded;

g. For declaratory relief; and

h. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury to the extent permitted by law.

DATED: November 15, 2017

FARUQI & FARUQI LLP

By: /s/ *Robert W. Killorin*

Robert W. Killorin
Georgia Bar No. 417775
3975 Roswell Road, Suite A
Atlanta, GA 30342
Telephone: (404) 847-0617
Facsimile: (404) 506-9534
Email: rkillorin@faruqilaw.com

Local Counsel

SPECTOR ROSEMAN & KODROFF, P.C.

Jeffrey L. Kodroff
John A. Macoretta
Daniel J. Mirarchi
1818 Market Street, Suite 2500
Philadelphia, PA 19103
Telephone: (215) 496-0300
Facsimile: (215) 496-6611
Email: jkodroff@srkattonreys.com
jmacoretta@srkattorneys.com
dmirarchi@srkattorneys.com

Attorneys for Plaintiff
Pro hac vice forthcoming

JS44 (Rev. 6/2017 NDGA)

CIVIL COVER SHEET

The JS44 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 is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

ANTHONY MIRARCHI, Individually and on Behalf of All Others Similarly Situated

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Philadelphia
(EXCEPT IN U.S. PLAINTIFF CASES)

DEFENDANT(S)

EQUIFAX, INC

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT Fulton County
(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, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

Robert W. Killorin, rkillorin@faruqilaw.com
FARUQI & FARUQI, LLP
3975 Roswell Rd, Suite A
Atlanta, GA 30342
(404) 847-0617

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION

(PLACE AN "X" IN ONE BOX ONLY)

- ☐ 1 U.S. GOVERNMENT PLAINTIFF
- ☐ 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- ☐ 2 U.S. GOVERNMENT DEFENDANT
- ☑ 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES

(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

PLF	DEF		PLF	DEF	
☐ 1	☐ 1	CITIZEN OF THIS STATE	☐ 4	☑ 4	INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
☑ 2	☐ 2	CITIZEN OF ANOTHER STATE	☐ 5	☐ 5	INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
☐ 3	☐ 3	CITIZEN OR SUBJECT OF A FOREIGN COUNTRY	☐ 6	☐ 6	FOREIGN NATION

IV. 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 District)
- ☐ 6 MULTIDISTRICT LITIGATION - TRANSFER
- ☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- ☐ 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

Class Action Fairness Act, 28 U.S.C. § 1332(d)(2); Willful Violation of The Fair Credit Reporting Act ("FCRA"); Negligent Violation of FCRA; Negligence; Negligence Per Se; Breach of Covenant of Good Faith and Fair Dealing; Violation of the Georgia Fair Business Practices Act; Breach of the Georgia Security Breach Notification Act; Breach of Contract; Violation of the Georgia Declaratory Relief Act; Violation of Fed. Rule of Civ. P. 23;

(IF COMPLEX, CHECK REASON BELOW)

- ☑ 1. Unusually large number of parties.
- ☑ 2. Unusually large number of claims or defenses.
- ☐ 3. Factual issues are exceptionally complex
- ☑ 4. Greater than normal volume of evidence.
- ☑ 5. Extended discovery period is needed.
- ☐ 6. Problems locating or preserving evidence
- ☑ 7. Pending parallel investigations or actions by government.
- ☑ 8. Multiple use of experts.
- ☐ 9. Need for discovery outside United States boundaries.
- ☑ 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT $_____ APPLYING IFP _____ MAG. JUDGE (IFP) _____

JUDGE _____ MAG. JUDGE _____ NATURE OF SUIT _____ CAUSE OF ACTION _____
(Referral)

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK
- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK
- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☑ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 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 - "4" MONTHS DISCOVERY TRACK
- ☐ 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
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☐ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK
- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK
- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK
- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK
- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK
- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK
- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK
- ☐ 830 PATENT
- ☐ 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDA) - a/k/a Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK
- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK
- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK
- ☐ 375 FALSE CLAIMS ACT
- ☐ 376 Qui Tam 31 USC 3729(a)
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 490 CABLE/SATELLITE TV
- ☐ 890 OTHER STATUTORY ACTIONS
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK
- ☐ 410 ANTITRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK
- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☑ **CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23** **DEMAND $** over $5,000,000.00

JURY DEMAND ☑ **YES** ☐ **NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)**

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE See Attached **DOCKET NO.** See Attached

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)

- ☐ **1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☑ **2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.**
- ☐ **5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.**
- ☐ **6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):**

- ☐ **7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. , WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.**

SIGNATURE OF ATTORNEY OF RECORD **DATE**

JUDGE	DOCKET NO.
Hon. William S. Duffey, Jr.	1:17-cv-03422
Judge Amy Totenberg	1:17-cv-03433
Judge Thomas W. Thrash	1:17-cv-03436
Judge Mark H. Cohen	1:17-cv-03451
Judge Mark H. Cohen	1:17-cv-03444
Judge Charles A. Pannell, Jr	1:17-cv-03445
Judge William S. Duffey, Jr	1:17-cv-03463
Judge Amy Totenberg	1:17-cv-03456
Judge Leigh Martin May	1:17-cv-03443
Judge William S. Duffey, Jr	1:17-cv-03457
Judge Leigh Martin May	1:17-cv-03458
Judge Mark H. Cohen	1:17-cv-03459
Judge Eleanor L. Ross	1:17-cv-03460
Judge Charles A. Pannell, Jr	1:17-cv-03461
Judge William S. Duffey, Jr	1:17-cv-03447
Judge Amy Totenberg	1:17-cv-03448
Judge Steve C Jones	1:17-cv-03449
Judge Leigh Martin May	1:17-cv-03450
Judge Eleanor L. Ross	1:17-cv-03452
Judge Thomas W. Thrash, Jr	1:17-cv-03453
Judge William S. Duffey, Jr	1:17-cv-03454
Judge Amy Totenberg	1:17-cv-03476
Judge Charles A. Pannell, Jr	1:17-cv-03471
Judge Eleanor L. Ross	1:17-cv-03479
Judge Thomas W. Thrash, Jr	1:17-cv-03480
Judge Leigh Martin May	1:17-cv-03477
Judge Timothy C. Batten, Sr	1:17-cv-03482
Judge Amy Totenberg	1:17-cv-03483
Judge Timothy C. Batten, Sr	1:17-cv-03492
Judge Mark H. Cohen	1:17-cv-03497
Judge Eleanor L. Ross	1:17-cv-03498
Judge Thomas W. Thrash, Jr	1:17-cv-03499
Judge Thomas W. Thrash, Jr	1:17-cv-03501
Judge Timothy C. Batten, Sr	1:17-cv-03502
Judge Leigh Martin May	1:17-cv-03507
Judge Thomas W. Thrash, Jr	1:17-cv-03512
Judge William S. Duffey, Jr	1:17-cv-03509
Judge Eleanor L. Ross	1:17-cv-03523
Judge Steve C Jones	1:17-cv-03484
Judge Eleanor L. Ross	1:17-cv-03487
Judge Eleanor L. Ross	1:17-cv-03571
Judge Charles A. Pannell, Jr	1:17-cv-03578
Judge Steve C Jones	1:17-cv-03582
Judge Steve C Jones	1:17-cv-03708

JUDGE	DOCKET NO.
Judge Steve C Jones	1:17-cv-03764
Judge Charles A. Pannell, Jr	1:17-cv-03769
Judge William S. Duffey, Jr	1:17-cv-03745
Judge Mark H. Cohen	1:17-cv-03713
Judge Mark H. Cohen	1:17-cv-03659
Judge Charles A. Pannell, Jr	1:17-cv-03586
Judge Eleanor L. Ross	1:17-cv-03613
Judge Leigh Martin May	1:17-cv-03676
Judge Steve C Jones	1:17-cv-03518
Judge Amy Totenberg	1:17-cv-03798
Judge Leigh Martin May	1:17-cv-03765
Judge William S. Duffey, Jr	1:17-cv-04250
Judge Mark H. Cohen	1:17-cv-04389
Judge Charles A. Pannell, Jr	1:17-cv-03809
Judge Leigh Martin May	1:17-cv-03872
Judge Amy Totenberg	1:17-cv-03587
Judge Leigh Martin May	1:17-cv-03829
Judge Clarence Cooper	1:17-cv-03863
Judge Clarence Cooper	1:17-cv-03881
Judge Timothy C. Batten, Sr	1:17-cv-03885
Judge Eleanor L. Ross	1:17-cv-03905
Judge Thomas W. Thrash, Jr	1:17-cv-03972
Judge Thomas W. Thrash, Jr	1:17-cv-04159
Judge Charles A. Pannell, Jr	1:17-cv-04544