IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF
GEORGIA ATLANTA DIVISION

ALCOA COMMUNITY FEDERAL CREDIT UNION, individually and on behalf of a class of all similarly situated financial institutions, Plaintiff. v. EQUIFAX, INC. Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

INTRODUCTION

1. On September 7, 2017, Equifax announced that hackers had exploited a vulnerability in Equifax's U.S. website to illegally gain access to consumers' highly sensitive personally identifiable information files.[1]

2. Plaintiff, Alcoa Community Federal Credit Union, ("Alcoa Credit Union" or "Plaintiff"), on behalf of itself and similarly situated banks, credit unions, and other financial institutions ("Class Plaintiffs"), that have suffered, and continue to suffer, financial losses and increased data security risks that are a direct result of Equifax's failure to safeguard the financial institutions' customers'

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

highly sensitive, personally identifiable information, alleges as follows based on (a) publicly available information; (b) personal knowledge of those matters relating to itself, and (c) upon information and belief as to all other matters, bring this putative class action against Equifax Inc. ("Equifax" or "Defendant").

NATURE OF THE CASE

3. Equifax collects and maintains highly sensitive, personally identifiable information, including, but not limited to, names, Social Security numbers, birth dates, addresses, and driver's license numbers ("PII") and payment card data, including, but not limited to, credit and debit card numbers, primary account numbers ("PANs"), card verification value numbers ("CVVs"), expiration dates and zip codes ("Payment Card Data") on over 820 million individual consumers and 91 million businesses.

4. Between at least May 2017 and July 2017, intruders gained access to the PII and payment card data of over 145.5 million U.S. consumers – roughly 44% of the United States population – as well as the Payment Card Data for an untold number of credit and debit cards in what was one of the largest data breaches in this country's history. To date, Equifax has reported up to 209,000

compromised consumer credit cards.[2]

5. Despite the well-publicized identification in March 2017, of the vulnerability in Apache Struts, and open-source application framework that supports Equifax online dispute portal web application, Equifax systematically failed to take reasonable steps to adequately protect the only product in which it exclusively trades and is responsible for protecting - the ultra-sensitive highly-sought-after personal and financial information of millions of individuals.[3]

6. Equifax's CEO admitted: "The company failed to prevent sensitive information from falling into the hands of wrongdoers. . .. [T]he breach occurred because of both human error and technology failures."[4]

7. The data breach was the inevitable result of Equifax's inadequate data security measures and approach to data security. Consequently, the financial

---

[2] AnnaMaria Andriotis, *et al., Equifax Hack Leaves Consumers, Financial Firms Scrambling*, FOXBUSINESS.COM (Sept. 8, 2017), www.foxbusiness.com/features/2017/09/08/Equifax-hack-leaves-consumers-financial-firms-scrambling.html.

[3] Dan Goodin, *Critical vulnerability under "massive" attack imperils high- impact sites*, ARSTECHNICA (Mar. 9, 2017), https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack- imperils-high-impact-sites/.

[4] Oversight of the Equifax Data Breach: Answers for Consumers: Hearing before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection (Oct. 3, 2017) (Prepared Testimony of Richard F. Smith), https://democrats-energycommerce.house.gov/ committee-activity/hearings/hearing-on-oversight-of-the-equifax-data-breach- answers-for-consumers ("Smith Testimony").

harms caused by Equifax's negligent handling of PII and Payment Card Data have been, and will be, borne in large part by the financial institutions that issue payment cards, process and hold various loans and credit products, and service accounts that are held by individuals whose PII and Payment Card Data has been compromised by the breach. These costs include, but are not limited to, canceling and reissuing an untold number of compromised credit and debit cards, reimbursing customers for fraudulent charges, increasing fraudulent activity monitoring, taking appropriate action to mitigate the risk of identity theft and fraudulent loans and other banking activity, sustaining reputational harm, and notifying customers of potential fraudulent activity.

8. This class action is brought on behalf of financial institutions throughout the United States to recover the costs that they and others similarly situated have been forced to bear as a direct result of the Equifax data breach and to obtain appropriate equitable relief to mitigate future harm that is certain to occur in light of the unprecedented scope of this breach.

PARTIES

9. Plaintiff, Alcoa Community Federal Credit Union, is a not-for-profit financial cooperative located in Benton, Arkansas. As a result of the Equifax data breach, Plaintiff has suffered injury, including, *inter alia*, costs to increase

fraudulent activity monitoring, costs to take appropriate action to mitigate the risk of identity theft and fraudulent loans and other banking activity, and costs due to sustaining reputational harm. Class Plaintiffs have suffered additional injury including costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs due to lost interest and transaction fees due to reduced card usage and for notifying customers of potential fraudulent activity as the result of the admitted compromise of at least 209,000 consumer credit cards.

10. Defendant Equifax Inc. is a publicly traded corporation with its principal place of business at 1550 Peachtree Street NE, Atlanta, Georgia. Equifax is one of the largest consumer credit reporting agencies in the United States gathering, analyzing, and maintaining credit-reporting information on over 820 million individual consumers and over 91 million businesses.

JURISDICTION AND VENUE

11. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because at least one Class member is of diverse citizenship from one defendant, there are more than 100 Class Plaintiffs, and the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs.

12. This Court has personal jurisdiction over Defendant because it maintains its principal headquarters in Georgia, is registered to conduct business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Defendant intentionally avails itself of this jurisdiction by conducting its corporate operations here and promoting, selling, and marketing Equifax products and services to resident Georgia consumers and entities.

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

FACTUAL ALLEGATIONS

Background

14. Equifax was founded in 1899 and is the oldest and second-largest consumer credit reporting agency in the United States. Equifax has over $3 billion in annual revenue, and its common stock is traded on the New York Stock Exchange under the ticker symbol "EFX."

15. Equifax's 2016 Form 10-K states that it "is a leading global provider of information solutions and human resources business process outsourcing services for businesses, governments and consumers. We have a large and diversified group

of clients, including financial institutions, corporations, governments and individuals. Our 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. We use advanced statistical techniques and proprietary software tools to analyze all available data, creating customized insights, decision-making solutions and processing services for our clients."[5]

16. For consumer files, Equifax collects a substantial amount of sensitive personal information regarding individual consumers and businesses from companies that have extended credit to consumers in the past, currently extend credit to consumers, or who wish to extend credit to consumers. Equifax's consumer credit files include individual's names, current and past addresses, birth dates, social security numbers, and telephone numbers; credit account information, including the institution name, type of account, date account was opened, payment history, credit limit, balance; credit inquiry information, including credit applications; and public-record information, including liens, judgments and bankruptcy filings. Credit card companies, banks, credit unions, retailers, and

[5] https://investor.equifax.com/~/media/Files/E/Equifax-IR/documents/financial-information/form-10-k.pdf (last accessed Oct. 3, 2017).

auto and mortgage lenders all report the details of consumer credit activity to Equifax.[6]

17. In addition, Equifax obtains PII and Payment Card Data directly from consumers who purchase credit reporting, monitoring, and other products from Equifax.

18. Armed with this data, Equifax analyzes the information that it collects and generates consumer credit reports, which it sells to businesses like retailers, insurance companies, banks and financial institutions like the Plaintiff, and government agencies. Equifax sells four primary data products: credit services, decision analytics, marketing, and consumer assistance services:

a. **Credit Services.** Equifax generates consumer credit reports that are purchased and reviewed by lending institutions, like the Plaintiff, to assist in making decisions about whether credit should be extended and in what amount.

b. **Decision Analytics.** Equifax also packages detailed transaction histories with analytics about the ways an

[6] *How Do Credit Reporting Agencies Get Their Information?* (July 2, 2014), https://blog.equifax.com/credit/how-do-credit-reporting-agencies-get-their- information/.

individual interacts with certain debt. Credit issuers pay more for these reports, as they offer a deeper analysis of the appropriateness of certain credit for certain consumers.

c. **Marketing**. Credit issuers that offer pre-approved credit pay a marketing fee to Equifax for a list of consumers who meet predetermined requirements. This information is used to extend offers of credit to consumers who meet an institution's desired criteria.

d. **Consumer Services.** Equifax also provides services directly to consumers, including credit monitoring and identity-theft- protection products. Additionally, Equifax is required by law to provide one free annual credit report to consumers.

19. Equifax has an obligation - an established and clear legal duty - to use every reasonable measure to protect the sensitive information that it collects and possesses from exposure to hackers and identity thieves.[7]

[7] *See*, *e.g.*, Fair Credit Reporting Act, 15 U.S.C. §1681(a)(4) and (b).

Plaintiff Relied on Equifax to Adequately Protect Customer's Sensitive Information

20. When the Plaintiff provides Equifax with its customers' most sensitive information, or when Equifax comes by such information in some other manner, the Plaintiff reasonably expects that Equifax will properly secure its website from hackers and that customers' information will be maintained and stored by Equifax in a safe and confidential manner, using all reasonable safeguards and protections. The potential harm from doing otherwise is obvious to Equifax, which knows that the Plaintiff, as a payment card issuer and lender, bears the ultimate responsibility for identity theft and fraudulent lending and consumer transactions.

21. Generally, financial institutions like Plaintiff report to the credit reporting bureaus, including Equifax, on a monthly basis. Plaintiff provides this confidential information to Equifax so that Equifax may use its expertise to aggregate, process, and analyze the information, so it can then be marketed to the financial services industry and to consumers directly. Equifax had a duty to properly secure its IT systems and website from hackers, to use available technology to encrypt and otherwise secure consumers' personal information using industry standard methods, and to act reasonably to prevent the foreseeable harm to

Plaintiff and the Class, which it reasonably should have known would result from a data breach.

22. Indeed, Equifax's role as a credit-reporting firm made the need for it to secure the information it held especially acute. And that role has itself created an additional burden for financial institutions, which have typically relied on the files at credit-reporting agencies, such as Equifax, to determine whether applications for consumer credit or loans are creditworthy. Not only has that process now been thrown into jeopardy for the Plaintiff and the Class they seek to represent, but also such financial institutions are now without a reliable, vital source of verifying consumers' identities due to the extent of the personal and financial information compromised by the Equifax breach.[8]

23. Taking advantage of Equifax's lax data security and delayed notification to consumers and financial institutions, hackers were able to gather large amounts of consumer data. With that data, unknown perpetrators are able to make hundreds of thousands or even millions of fraudulent undetected purchases on credit and debit cards that had been issued by

[8] *See* Telis Demos, *Equifax Hack Could Slow Down Fast Loans*, WALL STREET JOURNAL, Sept. 11, 2017, https://www.wsj.com/articles/equifax-hack-could-slow- down-fast-loans-1505147969.

members of the Class. Unknown perpetrators may also target and drain debit accounts with large amounts of money in them, concentrating the damages and causing individual financial institutions, such as Plaintiff and members of the Class, significant losses. Indeed, given the duration of the Equifax data breach—approximately two months—hackers appeared to have had near unfettered access to significant consumer data.

24. Equifax failed to acknowledge that its systems had been subjected to a breach, occurring from approximately May 2017 to July 2017, until September 7, 2017.

25. The dire consequences Equifax's failure to secure and maintain its data cannot be overemphasized. With the information used to establish a legal identity now available to identity thieves for over 145 million consumers, lenders are at a greatly increased risk of loan fraud and payment card transaction fraud, and are left to devise and implement, and pay for, their own prophylactic measures to reduce such risk.

26. For all of these reasons, the breach has sent shockwaves throughout the entire financial services industry, and its reverberations will be felt for years to come, each of which will inflict injury and damages upon financial institutions such as the Plaintiff and members of the proposed class.

The Equifax Data Breach

27. On September 7, 2017, Equifax announced a data breach event estimated to affect approximately 143 million U.S. consumers.

28. From at least May 13, 2017 to July 30, 2017, hackers exploited vulnerability in Equifax's U.S. web server software to illegally gain access to certain consumer files. The attack vector used in this incident occurred through a vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application.[9]

29. The potential vulnerability of the Apache Strut software was no secret. Security researchers with Cisco Systems, Inc. warned in March 2017 that a flaw in the Apache Struts software was being exploited in a "high number" of cyber-attacks.[10] Numerous other entities also identified and issued public warnings in March 2017 regarding the vulnerability, including The Apache Foundation, the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST"), and the U.S. Department of Homeland Security's Computer Emergency

---

[9] Equifax, *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes* (Sept. 15, 2017), https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/.

The alleged May 13, 2017 start date is based on Equifax's public statements of the results of its own investigation. Other sources, including Visa and MasterCard, have suggested that the breach may have started much earlier, as far back as November 2016.

[10] Andriotis, *supra* note 2.

Readiness Team ("U.S. CERT"). Apache and NIST described the flaw as "critical," which is the highest rating those groups use to indicate the danger of a vulnerability. In the days that followed, media reports noted that hackers were already exploiting the vulnerability against various companies and government agencies.[11] Equifax has publicly stated that its security team "was aware of this vulnerability at that time [in March 2017]."[12]

30. Even prior to the announcement of the exploitation by hackers of the flaw in the Apache Strut software, numerous data breaches had occurred at large retailers and restaurants nationwide, including Wendy's, Home Depot, Target, KMART, P.F. Chang's, and many others. Despite the increasing occurrences of data breaches of systems, and the specific notice of a vulnerability in their IT systems Equifax refused to take steps to adequately protect its computer systems from intrusion, continuing to use the Apache Strut software for two and a half months without properly applying the available patches or taking other measures to protect against the flaw.[13]

---

[11] Dan Goodin, *supra* note 3.

[12] *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* note 2.

[13] Elizabeth Weise and Nathan Borney, *Equifax Had Patch 2 Months Before Hack and Didn't Install It, Security Group Says*, USA TODAY (Sept. 14, 2017), http://www.usatoday.com/story/money/2017/09/14/equifax-identity-theft-hackers-apache-struts/665100001/

31. On March 7, 2017, the same day the vulnerability was publicly announced, The Apache Foundation made available various patches and workarounds to protect against the vulnerability.[14]

32. Specifically, on March 8, 2017, U.S. CERT sent Equifax a notice of the need to patch a particular vulnerability in the "Apache Struts" software used for its online disputes portal, where consumers can dispute items on their credit report.[15]

33. Equifax admitted that although it disseminated the U.S. CERT notification on March 9, 2017, and requested that the Apache Struts software be patched, the Equifax security department did not patch the software in response to the March 9, 2017 notification. *Id*. Equifax further admits that it was this unpatched vulnerability in the Apache Struts software that allowed hackers to access PII.

34. Over the multi-month period of the Equifax Data Breach, hackers accessed sensitive consumer information, including names, social security numbers, birth dates, addresses, and driver's license numbers. The compromised data contains complete profiles of consumers whose personal information was

[14] *Id.*

[15] Smith Testimony at 2-3, *supra* note 4.

collected and maintained by Equifax.

35. In addition to accessing sensitive personal information, the hackers also accessed what Equifax purports to be 209,000 consumer credit card numbers, and an estimated 182,000 dispute records containing additional personal information.[16] Equifax stated that it believes all consumer credit card numbers were accessed in one fell swoop in mid-May 2017.

36. The hackers were also able to access Equifax's back-end servers, which are connected to financial institutions and enable the parties to share information digitally.[17]

37. Equifax estimates that 145.5 million Americans were impacted by this breach.[18] It has not speculated on the number of financial institutions put at risk by this breach, and has only admitted to losing Payment Card Data for roughly 200,000 payment cards. However, card brand alerts that inform card issuers, such

---

[16] Andriotis, *supra* note 2.

[17] Michael Riley, *et al., Equifax Suffered a Hack Almost Five Months Earlier Thant the Date It Disclosed*, BLOOMBERG.COM (Sept. 18, 2017), https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed?cmpid=socialflow-twitter-business&utm_content=business&utm_campaign=socialflow-organic&utm_source=twitter&utm_medium=social.

[18] Hamza Shaban, *Equifax says 2.5 million more may have been swept up in massive data breach*, WASHINGTON POST(Oct. 2, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/02/Equifax-says-2-5-million-more-may-have-been-swept-up-in-massive-data-breach/?utm_term=.f1f77ea141dd.

as Plaintiff, have started rolling in. These alerts already have revised the supposed beginning date of the breach from July 2017 all the way back to November 2016.

38. Equifax reportedly discovered this breach on July 29, 2017. [19]

39. After Equifax discovered the breach, but before Equifax disclosed it to the public on September 7, 2017, three high-level executives sold shares in the company worth nearly $1.8 million.[20] On August 1, just three days after Equifax discovered the breach, Equifax Chief Financial Officer John Gamble sold $946,374 worth of stock, and President of U.S. Information Solutions Joseph Loughran exercised options to sell $584,099 worth of stock. The next day, President of Workforce Solutions Rodolfo Ploder sold $250,458 worth of stock.

40. To date, Equifax has not explained its delay in reporting this breach to the public.

41. Equifax stated that on August 2, 2017, it hired the services of Mandiant, a cybersecurity firm, to internally investigate the breach.[21]

---

[19] *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes, supra* note 9.

[20] Anders Melin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed,* BLOOMBERG.COM (Sept. 7, 2017), https://www.bloomberg.com/news/articles/2017-09-07/three-equifaxexecutives-sold-stock-before-revealing-cyber-hack.

[21] *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* note 9.

42. After the breach was publicly revealed, Equifax created a website, www.equifaxsecurity2017.com, to enable consumers to check whether they were potentially impacted by the data breach. Once a consumer disclosed additional highly sensitive information to Equifax, namely their last name and last six digits of their social security number, Equifax would inform the consumer whether they had been impacted by the breach.

43. On the same page that informed the consumer whether they had been impacted or not, Equifax also directed consumers to a free identity theft protection and credit monitoring program, TrustedID,[22] they were offering in the wake of the breach. By signing up for TrustedID, consumers consented to settle all claims arising out of the use of TrustedID in arbitration, but retained their rights to trial of claims arising out of the data breach.

44. Starting on September 9, 2017, and commensurate with its ineptitude regarding data security, Equifax erroneously directed consumers to a spoof website at least four times via Twitter.[23] Rather than directing consumers to

[22] TrustedID is a wholly owned subsidiary of Equifax, whose data breach is the basis for this complaint.

[23] Janet Burns, *Equifax Was Linking Potential Breach Victims On Twitter To A Scam Site*, FORBES.COM (Sept. 21, 2017), https://www.forbes.com/sites/janetwburns/2017/09/21/equifax-was-linking-potential-breach-victims-on- twitter-to-a-scam-site/#bb68b87288f2.

www.equifaxsecurity2017.com to determine whether consumer sensitive information was potentially compromised, Equifax mistakenly directed its Twitter followers to www.securityequifax2017.com, a website that was created by swapping the two words around and whose sole purpose was to highlight the vulnerabilities of the website Equifax created to assist potential victims.

45. Federal regulators announced they were investigating Equifax's delayed notification about the breach. The FBI is also investigating the breach, and two congressional committees announced that they would hold hearings.[24]

46. On September 13, 2017, Visa issued a CAMS alert stating that it had been notified by an acquirer of a potential network intrusion at Equifax that has put Visa accounts at risk. The Visa CAMS alert indicated that the exposure window was approximately May 11, 2017 through July 26, 2017 and that the debit and credit card data that had been compromised included PAN, CVV2, expiration dates, and cardholder names. Visa further stated that financial institutions that received this CAMS alert should take necessary steps to prevent fraud and safeguard cardholders.[25]

47. On September 15, 2017, Equifax announced the retirements of its

[24] Andriotis, *supra* note 2.
[25] *See* Brian Krebs, *"Equifax Hackers Stole 200k Credit Card Accounts in One Fell Swoop"*, KREBS ON SECURITY, Sept. 14, 2017, https://krebsonsecurity.com/2017/09/equifax-hackers-stole-200k-credit-card-accounts-in-one-fell-swoop/comment-page-1/.

Chief Information Officer and Chief Security Officer in connection with the breach and its aftermath.[26]

48. Numerous states and state attorneys general have rebuked Equifax in the wake of the breach. On September 18, 2017, New York Governor Andrew Cuomo directed the state's Department of Financial Services to develop a rule forcing credit reporting agencies to register with the state and comply with its cybersecurity requirements.[27] On September 19, attorneys general from 43 states and the District of Columbia signed a letter to Equifax, criticizing Equifax for the data breach and its response.[28] The same day, Massachusetts Attorney General Maura Healey filed a suit against Equifax, seeking financial penalties and disgorgement of profits, alleging that the Company failed to promptly notify the public of the breach, failed to protect the personal data in its possession, and engaged in unfair and deceptive trade practices.[29]

---

[26] *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* note 9.

[27] Ashley Southall, *Cuomo Proposes Stricter Regulations for Credit Reporting Agencies*, NEW YORK TIMES (Sept. 18, 2017), https://www.nytimes.com/2017/09/18/nyregion/equifax-hack-credit-reporting-agencies-regulations.html.

[28] Jack Suntrup, *Hawley, Madigan criticize Equifax in letter signed by other state attorneys general*, ST. LOUIS POST-DISPATCH (Sept. 19, 2017), http://stltoday.com/business/national-and-international/hawley-madigan-criticize-equifax-in-letter-signed-by-other-state/article_868a0dbf-1ec6-57e0-87a7-6d008005f8f0.html.

[29] David Lynch, *Equifax faces legal onslaught from US states*, FINANCIAL TIMES (Sept. 21, 2017), https://www.ft.com/content/bf04768c-9e1b-11e7-8cd4-932067fbf946.

49. On September 26, 2017, Equifax announced the abrupt retirement of its CEO, Richard Smith, less than three weeks after Equifax disclosed the data breach to the public and amid intense criticism of the Company.[30]

50. On October 2, 2017, Equifax announced that Mandiant had completed its internal forensic analysis of the data breach. Mandiant determined that an additional 2.5 million consumer records may have been compromised, bringing the total number of potentially compromised accounts to 145.5 million.[31]

51. This breach is one of the largest data breaches in history, due to both the number of people exposed and the sensitivity of the information compromised. As reported by the Wall Street Journal, "[t]he Equifax hack is potentially the most dangerous of all, though, because the attackers were able to gain vast quantities of personal identification— names, addresses, Social Security numbers and dates of birth—at one time."[32]

52. Upon information and belief, although many weeks have passed since Equifax discovered the breach, the investigation is still ongoing, and the identity of the hackers are still unknown.

---

[30] Hamza Shaban, *Equifax CEO Richard Smith steps down amid hacking scandal*, WASHINGTON POST (Sept. 26, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/26/equifax-ceo-retires-following-massive-data-breach/?utm_term=.995964f8571c.

[31] Hamza Shaban, *supra* note 18.

[32] Andriotis, *supra* note 2.

The Breach Was the Result of Equifax's Failure to Properly and Adequately Secure Its U.S. Website

53. Equifax disregarded the potential danger of a data breach by negligently failing to take adequate steps to prevent and stop hackers from gaining access to Equifax's computer systems.

54. The Equifax Data Breach was the direct result of Equifax's failure to properly and adequately secure its systems, which contained PII and card holder data.

55. Specifically, Equifax failed to heed warnings from security experts about the vulnerabilities in its Apache Strut software. Additionally, Equifax failed to update this software to its latest version. In a statement posted September 14, 2017, The Apache Software Foundation attributed the Equifax Data Breach to Equifax's "failure to install the security updates provided in a timely manner."[33]

56. Equifax admitted in public statements that hackers were able to access this data by exploiting vulnerability in Equifax's U.S. website application to illegally gain access to consumer files.

57. Equifax should have recognized and identified the flaws in its data security and should have taken measures to fix these vulnerabilities. Given the fact

[33] Id.; The Apache Software Foundation, MEDIA ALERT: The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for Apache Struts Exploit (Sept. 14, 2017),https://blogs.apache.org/foundation/entry/media-alert-the-apache-software.

the only product Equifax sells is highly sought-after data of the highest sensitivity, Equifax had a duty to employ up-to-the-minute data security and to use industry best practices to prevent a security breach.

58. Even before this incident, Equifax was on notice of potential problems with its web security. A security researcher has reported that in August, hackers claimed to have illegally obtained credit card information from Equifax, which they were attempting to sell in an online database.[34] Equifax had a duty to respond to such a report of a significant software security flaw. Despite Equifax's knowledge of these potential security threats, Equifax willfully (or at least negligently) failed to enact appropriate measures to ensure the security of its consumer files, including failing to encrypt sensitive personal and financial consumer information.

59. Specifically, as Equifax's CEO admitted, Equifax failed to reduce the scope of sensitive data retained in backend databases as well as failed to maintain adequate: vulnerability scanning and patch management processes and procedures; restrictions and controls for accessing critical databases; network segmentation between internet facing systems and backend databases and data stores; firewalls;

[34] Andriotis, *supra* note 2; *see also* Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES.COM (Sept. 8, 2017), https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#6b43b0ea677c.

file integrity monitoring; network, application, database, and system-level logging to monitor the network for unusual activity; and endpoint detection software to prevent exfiltration of data. [35]

60. The harm to Plaintiff resulting from Equifax's failure to adequately secure its computer systems and websites was at all times entirely foreseeable to Equifax.

61. Equifax is well aware of the costs and risks associated with payment card fraud and identity theft, and is particularly aware that Plaintiff and the Class bear the ultimate responsibility for payment card fraud and identity theft, as well as the obligation to protect against it. On its website, Equifax lists "some of the ways identity theft might happen," including when identity thieves "steal electronic records through a data breach."[36]

62. Because Equifax is aware of the harm caused by payment card fraud and identity theft, Equifax itself offers products aimed at protecting consumers from such illegal activity. For example, Equifax advertises its "Equifax Complete™ Premier Plan" as "Our Most Comprehensive Credit Monitoring and

[35] Smith Testimony, *supra* note 4.

[36] Equifax, *How Does Identity Theft Happen?* https://www.equifax.com/personal/education/identity-theft/how-doesidentity-theft-happen (last accessed Oct. 3, 2017).

Identity Protection Product."[37] The product promises to monitor consumers' credit scores, provide text message alerts when suspicious activity on consumer banking or credit card accounts occur, lock the consumer's credit file for unapproved third parties, and automatically scan suspicious websites for consumers' personal information.

63. Equifax was aware of the risk posed by its insecure and vulnerable website. It was also aware of the extraordinarily sensitive nature of the personal information that it maintains as well as the resulting impact that a breach would have on consumers and financial institutions – including Plaintiff and the other Class Plaintiffs.

Equifax Violated Federal Security Requirements and Other Industry Standards

64. The Equifax breach is unique because safeguarding consumer's highly sensitive personal information is one of the few responsibilities the company has, since sensitive data is the only product in which the company trades. As a company that deals exclusively in sensitive data, Equifax has a clear legal duty to maintain the confidentiality of consumer's sensitive information and prevent any third-party

[37] Equifax, *Equifax Complete™ Premier Plan: Our Most Comprehensive Credit Monitoring and Identity Protection Product*, https://www.equifax.com/personal/products/credit/monitoring-and-reports (last accessed Oct. 3,2017).

misuse or access to such information. Equifax's utter failure to safeguard consumer information violates federal data security standards and industry standards, as well as a clearly established legal duty to not act negligently when handling and storing PII and Payment Card Data.

Equifax Failed to Comply with Federal Trade Commission Requirements

65. According to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.[38]

66. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should a) protect the personal customer information that they keep; b) properly dispose of personal information that is no longer needed; c) encrypt information stored on computer networks; d) understand their network's vulnerabilities; and e) implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses a) consider using an intrusion detection system to expose a breach as soon as it occurs; b) monitor all incoming traffic for activity indicating someone may be trying to hack the system;

[38] Section 5 of 15 USC § 45 - https://www.law.cornell.edu/uscode/text/15/45

c) watch for large amounts of data being transmitted from the system; and d) have a response plan ready in the event of a breach.[39]

67. Another article "FTC Facts for Business" published by the FTC highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[40]

68. The FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

69. In the months and years leading up to the data breach and during the course of the breach itself, Equifax failed to follow the guidelines recommended by the FTC. Further, by failing to have reasonable data security measures in place, Equifax engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

Equifax Failed to Comply with Industry Standards for Data Security

70. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Data

[39] http://www.faegrebd.com/ftc-releases-data-security-guide-for-businesses

[40] https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf

Security Standard ("PCI DSS"). PCI DSS is the industry standard governing the security of payment card data, although it sets the minimum level of what must be done, not the maximum.[41]

71. PCI DSS 3.1, the version of the standards in effect at the time of the data breach, imposed the following twelve "high-level" mandates:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI DSS 3.1, furthermore, set forth detailed and comprehensive requirements that had to be followed to meet each of the twelve mandates.[42]

72. Among other things, PCI DSS required Equifax to properly secure payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; restrict access to payment card data to those with a need to know;

[41] https://www.pcisecuritystandards.org/
[42] https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf

establish a process to identify and timely fix security vulnerabilities; assign unique identification numbers to each individual with access to its systems; and encrypt payment card data at the POS.

Plaintiffs Have Been, Are Currently Being, and Will Be Harmed by the Equifax Data Breach

73. As a result of the Equifax's Data Breach, Plaintiff and Class Plaintiffs, to protect their customers and avoid fraud losses, have been forced to increase fraud monitoring on not only potentially impacted accounts but on all accounts, and to take other steps to protect themselves and their customers. In addition, Class Plaintiffs have been forced to cancel and reissue payment cards, change or close accounts, notify customers that their cards were compromised, investigate claims of fraudulent activity, and refund fraudulent charges. Class Plaintiffs have also lost interest and transaction fees due to reduced card usage. Furthermore, debit and credit cards belonging to Class Plaintiffs—as well as the account numbers on the face of the cards—were devalued.

74. Unlike other data breaches, however, the Equifax Data Breach has caused severe, long term damages in myriad other ways. Because Equifax provides services that are so core to the business functioning of credit extenders and lenders such as Plaintiff and members of the proposed class, the true extent of the damage may take years to fully materialize. Immediately, however, Plaintiff and members

of the proposed class are faced with the costs of dealing with customers who freeze their credit, making it impossible to determine their creditworthiness for current or potential credit or loans or to comply with regulatory requirements. Plaintiff and the Class are also faced with the requirement that in order to carry out their business functions, they must exchange the most sensitive customer information to a company that has proven to have no ability to secure data.

75. Furthermore, and perhaps most significantly, Plaintiff and the Class also face the obligation to pay for the costs of identity theft and fraudulent credit and other accounts for which the consumer victims are not responsible. The certain impending risk of identity theft and loan fraud as a direct result of the Equifax breach, and the protections which must be now put in place to limit such risks, represents significant harm to Plaintiff.

76. Equifax failed to follow industry standards and failed to effectively monitor its security systems to ensure the safety of customer information. Equifax's substandard security protocols and failure to adequately monitor for unauthorized intrusion caused consumers' PII and Payment Card Data to be compromised for months without detection by Equifax.

77. Furthermore, Plaintiff's and Class Plaintiffs' own data security is now at an increased and certain impending risk of being breached due to hackers

accessing Equifax's back-end servers.

78. Plaintiff has incurred and will continue to incur substantial damage because of Equifax's failures to meet reasonable standards of data security. Plaintiff has had to immediately take steps to prevent future fraud, including identity theft which will lead to loan fraud.

79. As a result of the Equifax data breach, Plaintiff is required to increase fraud monitoring on potentially impacted accounts, go to greater lengths to verify the identity of consumers seeking loans in light of impending credit freezes, and take other steps to protect itself and its customers, in an effort to reduce the risk of future, but certainly impending, identity theft, loan fraud, and other fraudulent consumer transactions. Additionally, Class Plaintiffs are required to cancel and reissue payment cards, change or close accounts, notify customers that their cards were compromised, investigate claims of fraudulent activity, and refund fraudulent charges.

80. Plaintiff and the Class also lost interest revenue and transaction fees due to reduced payment card usage and the account numbers on the face of the compromised cards were devalued.

81. Sensitive personal and financial information, like the information compromised in this breach, is extremely valuable to thieves and hackers. These

criminals have gained access to complete profiles of individuals' personal and financial information. They can now use this data to steal the identities of the consumers whose information has been compromised or sell it to others who plan to do so. The identity thieves can assume these consumers' identities (or create entirely new identities from scratch) to make transactions or purchases, open credit or bank accounts, apply for loans, forge checks, commit immigration fraud, obtain a driver's license in the member's or customer's name, obtain government benefits, or file a fraudulent tax return. A report by the Department of Justice found that 86% of identity theft victims in 2014 experienced the fraudulent use of existing account information, including credit card and bank account information.[43]

82. While consumers are ultimately protected from most fraud loss arising from this incident, Plaintiff and the Class are not, as they bear the primary responsibility for reimbursing customers for fraudulent charges, fraudulently opened accounts, and covering the costs of issuing new cards for customers to use. Additionally, Plaintiff and the Class will suffer financial losses whenever an identity is stolen and used to falsely establish credit. This certainly impending risk will continue into the foreseeable future, and will require Plaintiff and the Class to

[43] Erika Harrell, *Victims of Identity Theft, 2014*, U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS, NCJ 248991 (Sept. 2015) at 1, https://www.bjs.gov/content/pub/pdf/vit14.pdf.

incur significant costs and expenses in order to reduce and mitigate it.

83. Financial institutions are responsible for all charges to fraudulently opened accounts. When complete consumer profiles have been compromised, financial institutions experience continuous losses as identity thieves move on from one consumer profile to the next. With a breach of this magnitude, there is virtually no limit to the amount of fraudulent account openings financial institutions may face. These risks are very real in the wake of the Equifax breach and are certainly impending.

84. As a result of the Equifax data breach, financial institutions face considerable costs associated with monitoring, preventing, and responding to fraudulent charges and account openings. Financial institutions must implement additional fraud monitoring and protection measures, investigate potentially fraudulent activity, and indemnify members or customers for fraudulent charges. Financial institutions will also need to take other necessary steps to protect themselves and their members or customers, including notifying members or customers, as appropriate, that their accounts may have been compromised.

85. Consumers inevitably face significant emotional distress after theft of their identity. This stress also impacts financial institutions, which are forced to expend additional customer service resources helping their concerned customers.

Customers experiencing anxiety related to identity theft are often hesitant to use some banking services altogether, instead opting to use cash. As a result, financial institutions forgo many of the transaction fees, ATM fees, interest, or other charges that they may have otherwise collected on these accounts.

86. Financial institutions will also face increased regulatory compliance costs going forward as a result of this incident. Federal regulators have already begun considering the implications of the breach and are likely to implement additional requirements to protect consumers from the financial risks associated with this breach. For example, additional reports and plans will likely be required to satisfy regulators. Financial institutions will be required to directly bear the administrative costs of these additional measures.

87. Financial institutions are also harmed by the chilling effect this breach will have on future lending as consumers deal with the impact of the breach on their finances and credit. Customers or members are often without access to their accounts for several days at a time while credit or debit cards are replaced or accounts are changed. Additionally, some customers are hesitant to use card transactions altogether in the wake of a major breach. This results in lost fees and interest to the financial institutions issuing these cards.

88. Moreover, Equifax's massive and destabilizing data breach threatens

to severely disrupt the usual business operations of nearly every bank and credit union in the nation. This is because banks and credit unions rely upon Equifax to provide services that are core to the institutions' credit extension, lending, and other functions. The inability to reliably exchange the information that underlies these functions inflicts great, and real, risk and uncertainty to the financial institution's business models.

89. Even more worrisome, financial institutions are often required to demonstrate the health of their credit and loan portfolios to regulators, who require credit reports be pulled to analyze the strength of the portfolio. Such regulatory requirements cannot be met where great portions of consumers have implemented credit freezes, which are cumbersome and costly to switch on and off.

90. Ultimately, Plaintiff and the Class are faced with considerable present injury, and an immediate future of continually unfolding new and continued injuries as a result of Equifax's avoidable data breach.

Equifax Had a Clear Legal Duty to Prevent and Timely Report this Breach

91. Equifax had a legal duty to prevent a breach of consumers' sensitive personal information. This duty is also owed to the financial institutions which bear the readily foreseeable risk of injury.

92. Following several high-profile data breaches in recent years, including

Wendy's, Target, Home Depot and many others, Equifax was on notice of the very real risk that hackers could exploit vulnerabilities in its data security. Moreover, Equifax has considerable resources to devote to ensuring adequate data security.

93. Nonetheless, Equifax failed to invest in adequate cyber security measures to properly secure its U.S. website from the threat of hackers.

94. Financial institutions were harmed not only by the breach itself, but also by Equifax's failure to timely report this breach to the public.

95. Equifax discovered this breach on July 29, 2017, but did not report it to the public until nearly six weeks later, on September 7, 2017.

96. According to one report, an anonymous source familiar with the investigation states that "Equifax executives decided to hold off on informing the public until they had more clarity on the number of people affected and the types of information that were compromised."[44] But Equifax has not yet given an official explanation for its delay in reporting this breach to the public. In the time between when Equifax discovered this breach and when it reported the breach to the public, however, three of its top executives sold substantial sums of stock in the company, presumably avoiding the financial losses associated with the negative press

[44] *Id.*

Equifax has received since the breach.[45]

97. Because of this delay, consumers with compromised personal information and credit card information have been unable to adequately protect themselves from potential identity theft for several weeks. The consequences to financial institutions from this delay are very real, given that they ultimately bear financial responsibility for the fraud inflicted upon consumers.

98. Financial institutions have been unable to alert their members or customers of the risk in a timely manner, or to implement measures to detect and prevent potential fraud in the time before the breach was disclosed. The failure of Equifax to report the breach in a timely manner has resulted in additional harm to Plaintiff and the Class.

Equifax Has a History of Poor Data Security

99. Even before the 2017 data breach, Equifax was on notice of potential problems with its web security and has suffered from multiple security breaches in the past.

100. In April of 2016, it was revealed that hackers were able to exploit Equifax's W-2Express website, an Equifax service for companies to make

[45] Equifax's stock prices dropped almost 15% the day after the breach was publicly announced—the largest decline in nearly two decades. Ben Eisen, *Equifax Shares on Pace for Worst Day in 18 Years*, WALL STREET JOURNAL (Sept. 8, 2017), https://blogs.wsj.com/moneybeat/2017/09/08/equifaxshares-on-pace-for-worst-day-in-18-years/.

electronic W-2 forms accessible to employees, and accessed employees' sensitive tax data. Through an online portal, the hackers only had to enter an employee's default PIN code, which was simply the last four digits of the employee's Social Security number, and the employee's four-digit birth year. More than 400,000 employees' W-2 tax information was subsequently left open to theft.[46]

101. The use of simple and easily identifiable information for a default login and password to access sensitive personal and financial data is a substandard security practice. Indeed, shortly after Equifax publicly announced the breach at issue, security researchers discovered that one of Equifax's online employee portals could be accessed by using the word "admin" for both the login and password. Once logged in through the portal, a user could easily access sensitive employee and consumer data.[47]

102. Security researchers have also questioned for years Equifax's use of an easily identifiable security PIN issued to consumers who have requested to lock their credit report. When a consumer requests a credit lock, Equifax provides a security PIN that the consumer can then later use to unlock their credit. Instead of providing a secure, randomized PIN, Equifax only issues a date-time stamp of

[46] *See* Brian Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*, KREBS ON SECURITY, May 16, 2016, https://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/.

[47] See Brian Krebs, Auyda Help Equifax Has My Data, KREBS ON SECURITY (Sept. 17, 2017), https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/.

when the consumer requested the lock. Such an easily discernible PIN vastly increases the odds of someone attempting to unlock a credit report for the purposes of identity theft. Equifax has recently stated they are now taking steps to provide randomly generated PINs.[48]

103. The impact of such weak security practices often results in the exploitation of consumer information in the black market. As one security researcher reported, hackers claimed to have illegally obtained credit card information from Equifax, which they were attempting to sell in an online database.[49]

CLASS ACTION ALLEGATIONS

104. Plaintiff brings this action on behalf of itself and as a class action pursuant to the provisions of Rules 23(a) and 23(b)(3) of the Federal Rules of Civil Procedures on behalf of the following class (the "Class"):

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issue payment cards (including debit or credit cards) or

48 See Sean Gallagher, Equifax Moves To Fix Weak PINs For 'Security Freeze' On Consumer Credit Reports, ARSTECHNICA (Sept. 11, 2017), https://arstechnica.com/information-technology/2017/09/equifax-moves-to-fix- weak-pins-for-security-freeze-on-consumer-credit-reports/.

49 Andriotis, *supra* note 2; *see also* Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES (Sept. 8, 2017), https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-databreach-history/#63dc4270677c.

> perform, facilitate, or support other banking products and services, whose customers' and members' personal information was collected or amassed by Equifax and whose data was exposed in the 2017 breach of Equifax's U.S. website.

105. Excluded from the Class are Defendants and their subsidiaries and affiliates; all employees of Defendants; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned and his/her immediate family and his/her court staff.

106. Certification of Plaintiff's claims for class-wide treatment is appropriate because all elements of Fed. R. Civ. P. 23(a) and 23(b)(3) are satisfied. Plaintiff can prove the elements of its claims on a class-wide basis using the same evidence as would be used to prove those elements in an individual action alleging the same claims.

107. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believes that there are thousands or millions of members of the Class, the precise number of Class Plaintiffs is unknown to Plaintiff. Class Plaintiffs may be identified through objective means. Class Plaintiffs 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.

108. **Commonality and Predominance:** All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class Plaintiffs, including, without limitation:

a. Whether Equifax engaged in the misconduct alleged herein;

b. Whether Equifax owed a duty to Plaintiff and Class Plaintiffs to protect cardholder personal and financial data against unauthorized access;

c. Whether Equifax failed to provide adequate security to protect consumer cardholder personal and financial data from unauthorized access;

d. Whether Equifax negligently or otherwise improperly allowed cardholder personal and financial data to be accessed by third parties;

e. Whether Equifax failed to adequately notify Plaintiff and Class Plaintiffs that its data systems were breached;

f. Whether Equifax failed to adequately and, in a timely manner, contain or otherwise prevent hackers' access to customer data;

g. Whether Plaintiff and Class Plaintiffs were injured and suffered damages and ascertainable losses;

h. Whether Equifax's failure to provide adequate security proximately caused Plaintiff's and Class Plaintiffs' injuries;

i. Whether Plaintiff and Class Plaintiffs are entitled to damages and, if so, the measure of such damages; and

j. Whether Plaintiff and Class Plaintiffs are entitled to declaratory and injunctive relief.

109. **Typicality**: All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff is a member of the Class, having suffered injury including costs to increase fraudulent activity monitoring, costs to take appropriate action to mitigate the risk of identity theft and fraudulent loans and other banking activity, and costs due to sustaining reputation harm due to the Equifax data breach. Plaintiff's interests are not antagonistic to the claims of the other Class Plaintiffs, and there are no material conflicts with any other member of the Class that would make class certification inappropriate. Plaintiff and all members of the Class were damaged by the same

wrongful conduct of Equifax.

110. **Adequacy of Representation:** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff will fairly and adequately protect and represent the interests of the Class. The interests of the Plaintiff are coincident with, and not antagonistic to, those of the Class. Plaintiff is represented by counsel, who are competent and experienced in complex class action litigation of this type, and Plaintiff intends to prosecute this action vigorously. Plaintiff and its counsel will fairly and adequately protect the Class's interests.

111. **Predominance and Superiority:** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons or entities to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action.

112. Plaintiff knows of no special difficulty to be encountered in the

maintenance of this action that would preclude its maintenance as a class action.

COUNT I
Negligence
(On behalf of Class Plaintiffs)

113. Plaintiff repeats and re-alleges each and every allegation contained above as if fully set forth herein.

114. Equifax owed – and continues to owe – a duty to Plaintiff and members of the Class, to use reasonable care in safeguarding PII and Payment Card Data and to notify them of any breach in a timely manner so that appropriate action can be taken to minimize or avoid losses. This duty arises from several sources, including, but not limited to, the sources described below, and is independent of any duty Equifax owed as a result of any of its contractual obligations.

115. Equifax has a common law duty to prevent the foreseeable risk of harm to others, including Plaintiff and the Class. That injury that would result from Equifax's failure to use reasonable measures to protect PII and Payment Card Data and to provide timely notice of a breach was foreseeable. It is well known that a common motivation of data breach perpetrators is the hackers' intentions to sell PII and/or Payment Card Data on underground black markets, and news outlets reported that this, in fact, occurred after the Home Depot and Target data breaches,

among others. Malicious or criminal attacks were the cause of 50% of the breaches covered by the IBM study, and were also the most costly.[50] It was also foreseeable that, if reasonable security measures were not taken, hackers would steal PII and Payment Card Data belonging to millions; thieves would use the PII and Payment Card Data to make large numbers of fraudulent transactions; financial institutions would be required to mitigate the fraud such as by cancelling and reissuing the compromised cards and reimbursing their customers for fraud losses; and that the resulting financial losses would be immense.

116. Equifax owed, and continues to owe, a duty to protect others against the risk of foreseeable criminal conduct has been recognized in situations in which the parties are in a special relationship, or where an actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk. See Restatement (Second) of Torts, §302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard PII, Payment Card Data, and other sensitive information.

117. Only Equifax was in a position to ensure that its systems were sufficient to protect against the harm to financial institutions from a data breach.

[50] Identity Theft Resource Center, *Data Breach Reports:2016 End of Year Report* (Jan. 18, 2017), http://idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf.

118. Equifax assumed the duty to use reasonable security measures as a result of its conduct, internal policies and procedures, and Privacy Policy in which the company stated it was using "industry standard means" of protecting PII and Payment Card Data, and that its security measures were "appropriate for the type of information we collect." By means of these statements, Equifax specifically assumed the duty to comply with industry standards, including PCI DSS and every other conceivable standard applicable to a company whose sole business is transacting in the most sensitive consumer information there is.

119. A duty to use reasonable security measures also arises as a result of the special relationship that existed between Equifax and Plaintiff and the Class. The special relationship arises because financial institutions entrusted Equifax with customer PII and Payment Card Data. Only Equifax was in a position to ensure that its systems were sufficient to protect against the harm to financial institutions from a data breach.

120. Equifax's duty to use reasonable data security measures also arises under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by retailers such as Equifax. FTC publications

and data security breach orders further form the basis of Equifax's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

121. Equifax's duty to use reasonable care in protecting PII and Payment Card Data arises not only as a result of the common law and the statutes described above, but also because it was bound by, and had committed to comply with, industry standards, specifically including PCI DSS.

122. Equifax breached its common law, statutory and other duties, and thus was negligent, by failing to use reasonable measures to protect consumers' personal and financial information from the hackers who perpetrated the data breach and by failing to provide timely notice of the breach. Upon information and belief, the specific negligent acts and omissions committed by Equifax include, but are not limited to, some or all of the following:

a. failure to employ reasonable systems to protect against malware;

b. failure to regularly and reasonably update its antivirus software;

c. failure to maintain an adequate firewall;

d. failure to reasonably track and monitor access to its network and consumer data;

e. failure to reasonably limit access to those with a valid purpose;

f. failure to conduct frequent audit log reviews and vulnerability scans and remedy problems that were found;

g. failure to adequately staff and fund its data security operation;

h. Failure to use due care in hiring, promoting, and supervising those responsible for its data security operations;

i. failure to heed warnings about specific vulnerabilities in its systems identified by Equifax's own employees, consultants, and software vendors;

j. failure to recognize red flags signaling that Equifax's systems were inadequate and that, as a result, the potential for a massive data breach akin to the one involving Wendy's, Target and Home Depot was increasingly likely;

k. failure to recognize that for approximately eight months hackers were stealing PII and Payment Card Data from its systems while the data breach was taking place;

l. failure to contain the data breach or otherwise revoke hackers' access in a timely manner; and

m. failure to disclose the data breach in a timely manner;

123. As a direct and proximate result of Equifax's negligence, Plaintiff and members of the Class have suffered and continue to suffer injury, including but not limited to, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers, and other injuries as described herein. Class Plaintiffs have also suffered and continue to suffer injury, including but not limited to, cancelling and reissuing payment cards, changing or closing accounts notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, lost interest and transaction fees due to reduced card usage resulting from the breach, and cards they issued (and the corresponding account numbers) rendered worthless.

124. Because no statutes of other states are implicated, Georgia common law applies to the negligence claims of Plaintiff and the Class.

COUNT II
Negligence
(On behalf of Class Plaintiffs)

125. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

126. Equifax had a continuing duty to Plaintiff, Class Plaintiffs, and Class Plaintiffs' customers, to use and exercise reasonable and due care in obtaining,

retaining, and safeguarding the personal and financial information of Plaintiff, other Class Plaintiffs, and Class Plaintiffs' customers.

127. Equifax owed a duty to Plaintiff and other Class Plaintiffs to take reasonable measures to provide adequate security to protect the personal and financial information of Plaintiff, other Class Plaintiffs, and Class Plaintiffs' customers. Because Equifax came into possession of the personal and financial information of Plaintiff's and other Class Plaintiffs' customers, Equifax had a duty to exercise reasonable care in safeguarding and protecting such information from being accessed, compromised and/or stolen by third parties.

128. Equifax breached its duties, allowed an unlawful, catastrophic intrusion into its computer system, failed to protect against such an intrusion, and allowed personal and financial information to be accessed, compromised and/or stolen by third parties.

129. Equifax had a duty to employ adequate and reasonable procedures for the safeguarding of the financial and personal information of Plaintiff's and other Class Plaintiffs' customers.

130. Equifax, through its acts and/or omissions, unlawfully breached its duty to Plaintiff and other Class Plaintiffs by failing to maintain adequate,

reasonable procedures designed to protect against unauthorized access and/or theft of financial and personal information

131. Equifax knew or should have known with the reasonable exercise of care of the risk inherent in retaining such information and the importance of providing adequate security.

132. Equifax breached its Arkansas common law, statutory and other duties, and thus was negligent, by failing to use reasonable measures to protect its customers' personal and financial information from the hackers, who perpetrated the data breach and by failing to provide timely notice of the breach. But for Equifax negligent and wrongful breach of its duties owed to Plaintiff and other Class Plaintiffs, financial and personal information would not have been accessed, compromised, and/or stolen.

133. As a direct and proximate result of Equifax unreasonable conduct, Plaintiff and other Class Plaintiffs have suffered substantial damages, which they seek to recover.

134. Further, Equifax actions were patently unreasonable with respect to the rights of the Plaintiff and other Class Plaintiffs. Equifax knew or should have known, in light of the surrounding circumstances that its negligence would naturally and probably result in damages to Plaintiff and other Class Plaintiffs.

Substantial, ongoing damages did result for Plaintiff and other Class Plaintiffs. Thus, punitive damages should be awarded to deter the actions of Equifax's and others who might engage in similar action or conduct.

COUNT II
Negligence Per Se
(On behalf of Class Plaintiffs)

135. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

136. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, 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 Customer Data. The FTC publications and orders described above also form the basis of Equifax's duty.

137. Equifax violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and Payment Card Data and by not complying with applicable industry standards, including PCI DSS. 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 major credit reporting agency, including specifically the immense damages that would result to consumers and financial institutions.

138. Equifax's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

139. Plaintiff and Class Plaintiffs are within the class of persons that Section 5 of the FTC Act (and similar state statutes) was intended to protect as they are engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. Moreover, many of the Class Plaintiffs are credit unions, which are organized as cooperatives whose members are consumers.

140. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty 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 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 injury, including but not limited to cost of increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their customers and other injuries as described herein. Additionally, Class Plaintiffs have and

continue to suffer injury including cancelling and reissuing payment cards, changing or closing accounts, notifying customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, and lost interest and transaction fees due to reduced card usage resulting from the breach. The cards they issued (and the corresponding account numbers) were rendered worthless.

142. Because no statutes of other states are implicated, Georgia common law applies to the negligence per se claim of Plaintiff and the Class.

COUNT III
Declaratory and Equitable Relief
(On behalf of All Plaintiffs)

143. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

144. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

145. An actual controversy has arisen in the wake of Equifax's data breach regarding its common law and other duties to reasonably safeguard its customers'

PII and Payment Card Data. Plaintiff alleges that Equifax's data security measures were inadequate and remain inadequate. Furthermore, Plaintiff continues to suffer injury and damages as described herein.

146. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Equifax owed and continues to owe a legal duty to secure PII and Payment Card Data and to notify financial institutions of a data breach under common law and Section 5 of the FTC Act, Card Operating Regulations, PCI DSS standards, its commitments, and various state statutes;

b. Equifax breached and continues to breach this legal duty by failing to employ reasonable measures to secure PII and Payment Card Data;

c. Equifax's breach of its legal duty proximately caused the data breach and caused harm to Plaintiff and the Class.

d. Equifax's ongoing breaches of its legal duty continues to cause Plaintiff harm.

147. The Court should also issue corresponding injunctive relief requiring Equifax to employ adequate security protocols consistent with industry standards

to protect PII and Payment Card Data. Specifically, this injunction should, among other things, direct Equifax to:

a. implement encryption keys in accordance with industry standards;

b. consistent with industry standards, engage third party auditors to test its systems for weakness and upgrade any such weakness found;

c. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

d. regularly test its systems for security vulnerabilities, consistent with industry standards; and

e. install all upgrades recommended by manufacturers of security software and firewalls used by Equifax.

148. If an injunction does not issue, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Equifax, which is a real possibility given the continued missteps taken by Equifax described herein, including using its official corporate communications to send affected consumers to phishing sites. Indeed, Equifax was hit with a separate data breach in

March 2017 that apparently did nothing to motivate the company to discover the other massive data breach going on at the same time.[51] The risk of another such breach is real, immediate, and substantial. If another breach at Equifax occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

149. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Equifax if an injunction is issued. Among other things, if another massive data breach occurs at Equifax, the Plaintiff and the Class will likely incur millions of dollars in damages. On the other hand, the cost to Equifax of complying with an injunction by employing reasonable data security measures is relatively minimal, and Equifax has a pre-existing legal obligation to employ such measures.

150. Issuance of the requested injunction will serve the public interest. Such injunction will serve the public interest by preventing another data breach at Equifax, thus eliminating the injuries that would result to Plaintiff, the Class, and the potentially millions of consumers whose confidential information would be

[51] Mark Coppock, *Equifax Confirms It Suffered A Separate Data Breach In March*, DIGITAL TRENDS (Oct. 3, 2017), https://www.digitaltrends.com/computing/equifax-data-breach-affects-143-million-american/.

compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court:

a. Certify the Class and appoint Plaintiff and Plaintiff's counsel to represent the Class;

b. Enter a money judgment in favor of Plaintiff and the Class to compensate them for the injuries suffered together with pre-judgment and post-judgment interest and treble damages and penalties where appropriate;

c. Enter a declaratory judgment as described herein;

d. Grant the injunctive relief requested herein;

e. Award Plaintiff and the Class reasonable attorneys' fees and costs of suit, as allowed by law; and

f. Award such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demand a trial by jury on all claims so triable.

Respectfully submitted this 7th day of November, 2017.

THE KHAYAT LAW FIRM

/s/ Robert C. Khayat, Jr.
Robert C. Khayat, Jr.
Georgia Bar No. 416981
rkhayat@khayatlawfirm.com
75 Fourteenth Street, N.E.
Suite 2750
Atlanta, Georgia 30309
Telephone: (404) 978-2750
Facsimile: (404) 978-2901

Michael L. Roberts
Karen Sharp Halbert
Susan M. Fowler
ROBERTS LAW FIRM, P.A.
20 Rahling Circle
PO Box 241790
Little Rock, AR 72223-1790
Telephone: 501-821-5575
Facsimile: 501-821-4474
mikeroberts@robertslawfirm.us

Charles Barrett
NEAL & HARWELL, PLC
1201 Demonbreun Suite 1000
Nashville, TN 37203
(615) 238-3647 (direct)
(615) 293-7375 (mobile)
cbarrett@nealharwell.com

Counsel for Plaintiff and the Proposed Class

LR 7.1(D) CERTIFICATE OF FONT COMPLIANCE

I hereby certify that the foregoing *Complaint* has been prepared with one of the font and point selections approved by the Court in Rule 5.1(C) of the Civil Local Rules of Practice for the United States District Court for the Northern District of Georgia, specifically Times New Roman 14 pt. font.

/s/ Robert C. Khayat, Jr.
Robert C. Khayat, Jr.
Georgia Bar No. 416981

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

UNITED STATES DISTRICT COURT

for the

Northern District of Georgia

ALCOA COMMUNITY FEDERAL CREDIT UNION, individually and on behalf of all similarly situated financial institutions,

Plaintiff(s)

v.

EQUIFAX, INC.

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Registered Agent: Shawn Baldwin, Esq.
1550 Peachtree Street. N.W.
Atlanta, Georgia 30309

A lawsuit has been filed against you.

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

Robert C. Khayat, Jr.
THE KHAYAT LAW FIRM
75 Fourteenth Street, Suite 2750
Atlanta, Georgia 30309
(404) 978-2750
rkhayat@khayatlawfirm.com

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

CLERK OF COURT

Date: 11/07/2017

Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

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

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

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

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

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

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

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

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

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)

ALCOA COMMUNITY FEDERAL CREDIT UNION, individually and on behalf of a class of all similarly situated financial institutions

DEFENDANT(S)

EQUIFAX, INC.

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Saline County, Arkansas
(EXCEPT IN U.S. PLAINTIFF CASES)

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT Fulton County, Georgia
(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 C. Khayat, Jr.
THE KHAYAT LAW FIRM
75 Fourteenth Street, Suite 2750
Atlanta, Georgia 30309
(404) 978-2750; rkhayat@khayatlawfirm.com

ATTORNEYS (IF KNOWN)

Registered Agent: Shawn Baldwin, Esq.
1550 Peachtree Street. N.W.
Atlanta, Georgia 30309

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)

This class action is brought on behalf of financial institutions throughout the United States to recover the costs that they and others similarly situated have been forced to bear as a direct result of the Equifax data breach and to obtain appropriate equitable relief to mitigate future harm that is certain to occur in light of the unprecedented scope of this breach.

(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 $** >$5,000,000

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

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE_____ **DOCKET NO.**_____

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.**

s/ Robert C. Khayat, Jr. 11/7/2017

SIGNATURE OF ATTORNEY OF RECORD **DATE**