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

LESLIE KATZ, BENJAMIN KATZ, and JOSEF KATZ, Individually and on Behalf of all Others Similarly Situated, Plaintiffs, vs. EQUIFAX, INC, Defendant.	**Civil Action No. _____** **COMPLAINT** **CLASS ACTION** **DEMAND FOR JURY TRIAL**

Plaintiffs Leslie Katz, Josef Katz, and Benjamin Katz (collectively referred to herein as the "Plaintiffs"), by and through their undersigned counsel, submit this Complaint on behalf of themselves and all others similarly situated. Plaintiffs' allegations are based upon their personal knowledge as to themselves and their own acts, and upon information and belief, developed from the investigation and analysis by Plaintiffs' counsel, including a review of publicly available information.

NATURE OF THE ACTION

1. Defendant Equifax, Inc. ("Equifax" or the "Company") is a global information solutions company used trusted unique data, analytics, technology and industry expertise to provide consumer credit reports to businesses, governments, and individuals for the purpose of allowing them to make more informed business and personal decisions. The Company organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers.

2. Equifax's reports are based on databases of consumer and business information derived from various sources, including credit, financial assets, telecommunications and utility payments as well as employment, income, demographic and marketing data. As part of its business, Equifax collects, stores and transmits the Class members' personal and proprietary information in their facilities and on its equipment, networks and corporate systems. In a manner which is legally required to protect the confidentiality of the information in the Company's possession.

3. From mid-May through July 2017, criminals exploited an Equifax U.S. website application vulnerability gaining unauthorized access to certain files. The accessed files included personal consumer information, such as names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers ("Personal Information"). In addition, the accessed files also included credit card numbers for approximately 209,000 consumers and certain dispute documents, which included personal identifying information, for approximately 182,000 consumers were accessed (which are also included in the definition of "Personal Information" herein).

4. On July 29, 2016, Equifax discovered that there was a breach in its security systems. However, Equifax would wait until September 7, 2017 to disclose in a press release the following information regarding this cybersecurity incident involving unauthorized access to certain consumer information (the "Breach"):

> Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately *143 million U.S. consumers*. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.

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. . . .

Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

"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," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The 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. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visit www.equifaxsecurity2017.com or contact a dedicated call center at 866-447-7559, which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. - 1:00 a.m. Eastern time.

5. Plaintiffs and other members of the Class and Subclasses, set forth below, face multiple and severe damages from such unauthorized access to their private Personal Information, including, but not limited to, the prospect of identity theft, illegal loss of their financial information, and improper access to credit card funds. They are now forced to incur out-of-pocket expenses and take the required steps necessary to protect themselves from the prospect of identity theft and other crimes which could be perpetrated against them with the use of their private Personal Information. In some cases, they may even need to take steps to remediate harm caused by criminals behind the Breach and resecure their identity and financial holdings.

6. Plaintiffs bring this class action against Equifax for its failure to adequately secure and protect the Personal Information of the Class and for failing to timely notify the Class that the security and confidentiality of their Personal Information stored on Equifax's computer system was compromised. Plaintiffs seek to recover damages caused to them and the Class and Subclasses by Equifax's violations of law, including state data breach statutes. Plaintiffs also seek injunctive relief requiring Equifax to properly safeguard the Class's Personal Information on its computer system or alternatively, remove such Personal Information from its computer system.

PARTIES

7. Plaintiff Leslie Katz is an individual consumer residing in the state of New York whose Personal Information has been compromised by Equifax's acts and/or omissions complained of herein. Plaintiff Leslie Katz received the following information from Equifax's website:

THANK YOU

> Based on the information provided, we believe that your personal information may have been impacted by this incident.
>
> Click the button below to continue your enrollment in TrustedID Premier.
>
> Enroll

For more information visit the FAQ page. (http://faq.trustedidpremier.com)

8. Plaintiff Benjamin Katz is an individual consumer residing in the state of Ohio whose Personal Information has been compromised by Equifax's acts and/or omissions complained of herein. Plaintiff Benjamin Katz received the following information from Equifax's website:

> THANK YOU
> Based on the information provided, we believe that your personal information may have been impacted by this incident.
>
> Click the button below to continue your enrollment in TrustedID Premier.
>
> Enroll
>
> For more information visit the FAQ page. (http://faq.trustedidpremier.com)

9. Plaintiff Josef Katz is an individual consumer residing in the state of New Jersey whose Personal Information has been compromised by Equifax's acts and/or omissions complained of herein. Plaintiff Josef Katz received the following information from Equifax's website:

> THANK YOU
>
> Based on the information provided, we believe that your personal information may have been impacted by this incident.
>
> Click the button below to continue your enrollment in TrustedID Premier.
>
> Enroll
>
> For more information visit the FAQ page. (http://faq.trustedidpremier.com)

10. Defendant Equifax is organized under the laws of the state of Georgia and maintains its principal executive offices at 1550 Peachtree Street, N.W., Atlanta, Georgia 30309.

In public filings with the Securities and Exchange Commission, Equifax describes its business as "a leading global provider of information solutions, employment and income verifications and human resources business process outsourcing services" that "leverage[s] some of the largest sources of consumer and commercial data, along with advanced analytics and proprietary technology, to create customized insights which enable our business customers to grow faster, more efficiently and more profitably, and to inform and empower consumers."

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 15 U.S.C. § 1681p of the Fair Credit Reporting Act. This Court also has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2), because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiffs and defendant Equifax are citizens of different states. The proposed Class and Subclasses each include well over 100 members.

12. This Court has personal jurisdiction over Equifax because the Company maintains its principal place of business in this District in Atlanta; regularly conducts business in Georgia; and has sufficient minimum contacts in Georgia. Equifax intentionally avails itself of this jurisdiction by marketing and selling products from Georgia to millions of consumers nationwide, including in the states of Ohio, New Jersey, and New York.

13. Venue is proper in this District pursuant to 28 U.S.C. §1391 because Equifax is a resident of this District and is subject to this Court's personal jurisdiction. Equifax is incorporated in Georgia, regularly conducts business in this District, and maintains its headquarters in this District. In addition, the causes of action arose, in substantial part, in this District.

FACTUAL ALLEGATIONS

14. Plaintiffs Leslie Katz, Benjamin Katz, and Josef Katz, are among the hundreds of millions of American consumers who have applied for a loan or credit card, ordered a credit report or their own use, or had their credit pulled for one reason or another. As a credit reporting agency, Equifax has therefore, in the course of their lives, compiled plaintiffs' sensitive and confidential Personal Information, including their social security numbers, birth dates, addresses, driver's license numbers and/or credit card numbers.

15. Equifax collected and stored Plaintiffs' Personal Information on its computer system, and used that information for its business activities and services for purposes of its own corporate profit.

16. Equifax owed a legal duty to Plaintiffs and all other U.S. consumers to use reasonable care to protect their credit and Personal Information from unauthorized access and/or acquisition by third parties. Equifax knew that failure to take the necessary cyber security measures to protect consumer credit and Personal Information from unauthorized access would cause serious risks of financial and credit harm and identify theft those consumers for years to come.

17. Despite this duty, Equifax negligently failed to maintain adequate technological and cyber security safeguards to protect the Personal Information of Plaintiffs and U.S. consumers from unauthorized access by hackers.

18. Equifax knew and should have known that failure to maintain adequate technological safeguards would eventually result in a massive data breach. Equifax could have and should have substantially increased the amount of money it spent to protect against cyber-attacks and other security breaches but chose not to in order to increase corporate profits.

19. Plaintiffs and members of the Class and Subclasses should not have to bear the expense caused by Equifax's negligent failure to properly safeguard their credit and Personal Information from cyber-attackers.

20. As a direct result of Equifax's negligence as alleged in this complaint, Plaintiffs and members of the Class and Subclasses now suffer serious risks of financial and credit harm and identify theft, and may do so for years to come.

21. Plaintiffs and members of the Class and Subclasses may also be required to expend out-of-pocket expenses for years to come in order to properly monitor their credit and financial property to ensure that no credit or financial wrongdoings or crimes of identity theft will be perpetrated against them.

22. Equifax has attributed the hack to a flaw in a type of code called Apache Struts, which is used by companies to develop web applications. According to Apache Software, the maker of Apache Struts, the flaw was exposed several months ago, in March, and "[t]he Equifax data compromise was due to their failure to install the security updates in a timely manner."[1]

23. Although Equifax discovered the Breach on July 29, 2017, the Company failed to disclose the Breach until September 7, 2017, approximately forty days later. Yet, in the interim, three executives of Equifax, including its Chief Financial Officer, were knowledgeable and opportunistic enough to take advantage of the Company's withholding of information regarding the Breach by selling a total of $2 million of Equifax stock in early August 2017.[2]

24. Even when it finally publically released the information, Equifax's disclosure of the Breach and notice to consumers was woefully deficient and inadequate. In particular, Equifax

[1] https://www.cnbc.com/2017/09/14/equifax-tumbles-as-ftc-confirms-investigation-into-breach.html

[2] https://www.cnbc.com/2017/09/07/equifax-cyberattack-three-executives-sold-shares-worth-nearly-2-million-days-after-data-breach.html

represented that its website would "indicate whether your personal information may have been impacted by this incident." After providing the required information, the consumer's last name and last six digits of his or her social security number, the website then only offered impacted consumers a statement noting that "[b]ased on the information provided, we be believe that your personal information *may* have been impacted by this incident." (Emphasis added.) No particulars as to what precise Personal Information of the consumer may have been compromised and the particular risk that posed is provided. Some consumers learned that the response from Equifax's website regarding the safety of their data would depend on what browser they were using or whether or not they accessed the website from a mobile device or a computer.[3] Moreover, consumers choosing to contact Equifax by phone to verify whether the Breach had impacted their Personal Information were simply advised to refer to the website, thereby leaving those without a secure internet connection unable to understand the status of their potentially compromised Personal Information. The Company also represented that it will provide affected consumers with an "option" to enroll in TrustedID Premier, a credit monitoring and identity theft protection service. However, many consumers who opted for this service have received a message that the user can only be enrolled in TrustedID Premier at a later date. In the days following the Company's notification regarding the Breach, it initially appeared that consumers who accepted the credit monitoring service offered by Equifax were initially forced to click through a statement inferring that an arbitration clause and class action waiver was attached to the TrustedID Service enrollment. Since then, and after the New York Attorney General Eric Schneiderman announced an investigation and was publically critical of the class action waiver,

[3] http://www.zdnet.com/article/we-tested-equifax-data-breach-checker-it-is-basically-useless/

Equifax clarified that consumers accepting services will *not* waive their consumer rights to a class action with regards to the cybersecurity incident that affected them.[4]

25. Most consumers, following the hack of Equifax's system, have sought to institute a credit freeze. A credit freeze allows consumers to restrict access to their credit report which makes it more difficult for identity thieves to open new accounts. There are three steps required to institute a credit freeze. First, a consumer must reach out to each of the three credit reporting agencies (Equifax, Experian, and TransUnion). Next, consumers ask each agency to institute a freeze on their credit report and supply the credit reporting agency with their name, address, date of birth, Social Security number and other personal information to confirm their identity. Finally, the consumer pays the credit reporting agency approximately $5-$10 to institute the freeze.[5]

26. Equifax, following the backlash from one of the largest data breaches in history, failed to ensure that they had adequate infrastructure so that consumers could freeze their credit and protect themselves from identity theft. In fact, two of the four Frequently Asked Questions ("FAQ") on Equifax's website for the data breach directly acknowledge that there are incredibly long wait time and frequent busy signals for consumers.[6] In addition, consumers that want to protect themselves by freezing their credit are facing a plethora of issues from Equifax including dead phone lines, incredibly long wait times, website errors.[7]

27. Adding to consumers' confusion, Equifax has also published a link to a phishing website. A phishing website is a website designed to look exactly like a legitimate business to steal visitors' personal information. Twice on September 9th and once on September 18th the

[4] https://www.cnbc.com/2017/09/08/new-york-attorney-general-launches-investigation-into-equifax-breach.html

[5] https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

[6] https://www.equifaxsecurity2017.com/frequently-asked-questions/#tab-2.

[7] *See e.g.*, https://www.nytimes.com/2017/09/14/reader-center/equifax-questions.html?mcubz=3; https://www.nytimes.com/2017/09/14/your-money/equifax-answers-data-breach.html?mcubz=3.

official Equifax twitter account told consumers they could visit www.securityequifax2017.com to enroll in Equifax's "TrustedID Premier" service. The actual website created by Equifax was www.equifaxsecurity2017.com. This further confused and harmed consumers that were looking for crucial information regarding the data breach.[8]

28. The severity of this data breach has led to investigations by state and federal authorities. On September 14, 2017 the Federal Trade Commission ("FTC") announced that they had begun an investigation into the data breach at Equifax.[9] The Massachusetts Attorney General has filed a lawsuit against Equifax.[10] The New York Attorney General, and Indiana Attorney General have launched formal investigations into the Equifax breach.[11]

CLASS ACTION ALLEGATIONS

29. Plaintiffs bring this class action and Counts I, II, III, IV, and V set forth below for willful and negligent violations of the Fair Credit Reporting Act, negligence, unjust enrichment, and declaratory judgment pursuant to the Federal Rules of Civil Procedure 23(a) and (b)(3), on behalf of themselves and a nationwide class of all others similarly situated in the United States.

The class is defined as follows:

> **Nationwide Class**:
> All residents of the United States whose Personal Information was compromised as a result of the data breach first disclosed by Equifax on September 7, 2017 (the "Class").

[8] https://www.nytimes.com/2017/09/20/business/equifax-fake-website.html?mcubz=3.

[9] https://www.cnbc.com/2017/09/14/equifax-tumbles-as-ftc-confirms-investigation-into-breach.html

[10] http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-09-19-equifax-lawsuit.html

[11] *See* http://www.indystar.com/story/news/crime/2017/09/22/indiana-attorney-general-curtis-hill-investigating-equifax-data-breach/693615001/; https://www.cnbc.com/2017/09/08/new-york-attorney-general-launches-investigation-into-equifax-breach.html

30. Pursuant to the Federal Rules of Civil Procedure, Rule 23, Plaintiff Benjamin Katz also brings Count VI set forth below on behalf of himself and an Ohio subclass of all others in Ohio similarly situated.

The Ohio subclass is defined as follows:

> **Ohio Statewide Class**:
> All residents of Ohio whose Personal Information was compromised as a result of the data breach first disclosed by Equifax on September 7, 2017 (the "Ohio Subclass").

31. Pursuant to the Federal Rules of Civil Procedure, Rule 23, Plaintiff Josef Katz also brings Count VII set forth below on behalf of himself and a New Jersey subclass of all others in New Jersey similarly situated.

The New Jersey subclass is defined as follows:

> **New Jersey Statewide Class**:
> All residents of New Jersey whose Personal Information was compromised as a result of the data breach first disclosed by Equifax on September 7, 2017 (the "New Jersey Subclass").

32. Pursuant to the Federal Rules of Civil Procedure, Rule 23, Plaintiff Leslie Katz also bring Count VIII set forth below on behalf of themselves and a New York subclass of all others in New York similarly situated.

The New York subclass is defined as follows:

> **New York Statewide Class**:
> All residents of New York whose Personal Information was compromised as a result of the data breach first disclosed by Equifax on September 7, 2017 (the "New York Subclass").

33. Excluded from the Class and Ohio, New Jersey, and New York subclasses (collectively, the "Subclasses") is Equifax and its parent or subsidiary companies, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, heirs, predecessors,

successors, assigns, legal representatives, agents, and employees. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

34. Each of the proposed classes meet the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3):

35. **Numerosity.** The proposed Class and Subclasses consist of potentially millions of persons whose data was compromised in the breach. While the precise number of members of the Class and Subclasses and the identities of individual members of the Class and Subclass are unknown to Plaintiffs' counsel at this time, and can only be ascertained through appropriate discovery, the massive size of the breach as well as the reported 143 million persons for whom Equifax collected Personal Information who may have been adversely affected, indicates that the membership of the Class and Subclass are each so numerous that joinder of all members is impracticable.

36. **Commonality.** Equifax's wrongful conduct affected all members of the Class and Subclasses in exactly the same way. Equifax's failure to properly safeguard the Class's Personal Information is completely uniform among the Class and Subclasses.

37. Questions of law and fact common to all members of the Class and Subclasses exist and predominate over any questions affecting only individual members. Such common questions of law and fact include:

a. Whether Equifax engaged in the conduct alleged herein;

b. Whether Equifax's actions constituted unfair methods of competition and unfair, deceptive, fraudulent, unconscionable trade practices actionable under Ohio, New Jersey, and New York consumer fraud statutes;

c. Whether Equifax owed a duty to members of the Class and Subclasses to protect their Personal Information;

d. Whether Equifax acted wrongfully and/or breached its legal duties by failing to properly secure and safeguard the Personal Information of members of the Class and Subclasses stored on in its computer system;

e. Whether Equifax had a legal duty to provide timely and accurate notice of the breach to Plaintiffs and Class members;

f. Whether Equifax breached its legal duty to provide timely and accurate notice of the breach to Plaintiffs and Class members;

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

h. Whether the Plaintiffs and the other members of the Class and Subclasses have been damaged by Equifax's breach of its legal duties, and, if so, what is the appropriate relief.

38. **Typicality**. The Plaintiffs' claims, as described herein, are typical of the claims of all other members of the Class and Subclasses, as the Plaintiffs and all other members of the Class and Subclasses were injured through Equifax's uniform misconduct and the legal claims arise from the same set of facts regarding the Defendant's failure to protect the Class and Subclasses member's Personal Information. The Plaintiffs maintain no interest antagonistic to the interests of other members of the Class or Subclasses.

39. **Adequacy.** Plaintiffs are committed to the vigorous prosecution of this action and has retained competent counsel experienced in the prosecution of class actions of this type. Moreover, Plaintiffs interests do not conflict with the interests of the members of the Class and

Subclasses whom they seek to represent. Accordingly, the Plaintiffs are adequate representatives of the Class and Subclasses and will fairly and adequately protect their interests.

40. **Superiority.** A class action is superior to all other available methods of fairly and efficiently adjudicating the claims of the Plaintiffs and the Class and Subclasses for the following reasons:

a. common questions of law and fact predominate over any question affecting any individual members of the Class and Subclasses;

b. the injury sustained by each member of the Class and/or Subclasses, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Equifax;

c. even if it were economically feasible, the prosecution of separate actions by individual members of the Class and Subclasses would likely impose a crushing burden on the court system and create a risk of inconsistent or varying adjudications with respect to individual members, while, in contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court;

d. the proposed Class and Subclasses are well defined and all members of the Class and Subclasses are readily ascertainable, as Equifax has access to their identifying Personal Information, including, but not limited to, names, addresses, and/or other contact information which can be used to identify and contact members of the Class and Subclasses;

e. this forum is appropriate for litigation of this action since a substantial portion of the transactions, acts, events, and omissions alleged herein occurred in this District; and

f. prosecution as a class action will eliminate the possibility of repetitious litigation, while also providing redress for claims that may be too small to support the expense of individual, complex litigation.

41. For these reasons, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

COUNTS

FIRST CAUSE OF ACTION

Willful Violation of the Federal Fair Credit Reporting Act (15 U.S.C. § 1681a(c))

42. Plaintiffs incorporate all preceding and subsequent paragraphs by reference.

43. Plaintiff and the Class members are consumers entitled to the protections of the Fair Credit Reporting Act, 15 U.S.C. 1681a(c) ("FCRA")

44. 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).

45. 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.

46. 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).

47. 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.

48. 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 Class members' information. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

49. Equifax furnished 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.

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

51. 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 willfully failed to take them.

52. 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 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 Plaintiffs and other members of the Classes of their rights under the FCRA.

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

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

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

SECOND CAUSE OF ACTION

Negligent Violation of the Fair Credit Reporting Act
(15 U.S.C. § 1681 (a)(c))

56. Plaintiff incorporates all preceding and subsequent paragraphs by reference.

57. 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 past data breaches. 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.

58. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and Class members' information and consumer reports for no permissible purpose under the FCRA.

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

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

THIRD CAUSE OF ACTION

Negligence

61. Plaintiffs incorporate and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.

62. Equifax owed a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Personal Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Equifax's computer network security systems, along with the use of reasonable and adequate security procedures and systems consistent with industry standard practices, to ensure that Plaintiffs and the other members of the Class' Personal Information in Equifax's possession were adequately secured and protected. Equifax further owed a duty to Plaintiffs and the other members of the Class to implement processes that would timely detect a breach of its computer security and to prevent mass exports of Personal Information out of Equifax's computer network.

63. Equifax owed a duty of care to Plaintiffs and the other members of the Class because there was a reasonable expectation that Equifax would keep that information secure and confidential. Equifax solicited, gathered, and stored the Personal Information for its own business purposes, and, in the absence of negligence, would have known that by holding massive amounts of Personal Information it was an attractive target for hackers, and that proper security measures were necessary to prevent a breach of its computer security systems and the stealing of personal data which would damage Plaintiffs and the other members of the Class. Because members of the Class were foreseeable and probable victims of any inadequate information security practices, Equifax had a duty to adequately protect such the Class's Personal Information from hackers.

64. Equifax also owed a duty to Plaintiffs and the other members of the Class to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

65. In the case of a data breach, Equifax owed a duty Plaintiffs and the other members of the Class to timely and accurately disclose that their Personal Information had been improperly acquired or accessed so that Plaintiffs and members of the Class could take immediate action to mitigate the risk and damage caused by such a data breach.

66. Plaintiffs and other members of the Class relied on Equifax to safeguard their Personal Information that it collected, used and stored and was in a unique position to (and capable of) protecting against the harm caused to Plaintiffs and the other members of the Class as a result of the Breach.

67. Equifax's conduct created a foreseeable risk of harm to Plaintiffs and the other members of the Class. Equifax's misconduct included, but was not limited to, its failure to take

the steps and opportunities to effectively encrypt, and then to prevent and stop the Breach, and to timely detect and disclose the Breach as set forth herein.

68. Equifax breached the duties it owed to Plaintiffs and the other members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiffs the members of the Class.

69. Equifax breached the duties it owed to Plaintiffs and the other members of the Class by failing to properly implement technical systems or security practices that could have prevented the loss of the confidential data at issue.

70. Equifax breached the duties it owed to Plaintiffs and the other members of the Class to timely and accurately disclose that their Personal Information had been improperly acquired or accessed during the course of the breach so that Plaintiffs and members of the Class could take immediate action to mitigate the risk and damage caused by such a data breach.

71. As a direct and proximate result of Equifax's conduct, Plaintiffs and the other members of the Class were injured by Equifax's breach of these duties and suffered damages including, but not limited to, loss of control of their Personal Information, an added burden and cost of heightened monitoring for signs for identity theft and for undertaking actions such as credit freezes and alerts to prevent identity theft, and remediating acts and damages caused by identity theft, the inability to properly monitor their personal credit, financial assets, and identity from improper use and identity theft until approximately forty days following the Breach, and other economic damages.

FOURTH CAUSE OF ACTION

Unjust Enrichment

72. Plaintiffs incorporate and re-allege the allegations contained in the preceding and subsequent paragraphs as if fully set forth herein.

73. Plaintiffs and members of the Class or, alternatively, the Subclasses (collectively, the "Class" as used in this Count), had their Personal Information collected and used by Equifax as part of the business services and/or products. The use of their Personal Information conferred a monetary benefit on Equifax.

74. Equifax knew that the use of Plaintiffs' and the Class's information conferred a benefit on Equifax, and it thereby profited by using their Personal Information for its own business purposes.

75. Equifax failed to secure the Plaintiffs' and Class members' Personal Information, and acquired the Personal Information through inequitable means because it failed to disclose the inadequate security practices previously alleged.

76. Had Plaintiffs and Class members known that Equifax would not secure their Personal Information using adequate security, they would have requested Equifax destroy or not retain such information.

77. Plaintiffs and the Class have no adequate remedy at law.

78. Under the circumstances, it would be unjust for Equifax to be permitted to retain any of the benefits that Plaintiffs and Class members' Personal Information conferred on it, particularly given the inequitable and fraudulent pretenses under which it was attained.

79. Equifax should be compelled to disgorge into a common fund or constructive trust for the benefit of the proceeds it received from processing and selling Plaintiffs and Class members' Personal Information.

FIFTH CAUSE OF ACTION

Declaratory Judgment

80. Plaintiffs incorporate and re-allege the allegations contained in the preceding and subsequent paragraphs as if fully set forth herein.

81. Equifax owed duties of care to Plaintiffs and the members of the Class or, alternatively, the Subclasses that require it to adequately secure Personal Information.

82. Equifax still possesses Personal Information of the Plaintiffs and members of the Class.

83. After the Breach, Equifax announced changes that it claimed would improve data security. These changes, however, did not fix many systemic vulnerabilities in Equifax's computer systems. A "FAQ" posted to https://www.equifaxsecurity2017.com/frequently-asked-questions/ states that "to prevent this from happening again" Equifax has "engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again."

84. Accordingly, Equifax still has not satisfied its obligations and legal duties to Plaintiffs and the Class members.

85. Actual harm has arisen in the wake of the breach and Equifax's failure to properly provide security measures to Plaintiffs and the members of the Class and Subclasses. Equifax does not maintain that its security measures now are adequate to meet Equifax's legal duties.

86. Plaintiffs, therefore, seek a declaration (a) that Equifax's existing security measures do not comply with its legal duties to provide adequate security, and (b) that to comply with its obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to: (1) 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; (2) ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring; (3) ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Equifax segment Class members' data by, among other things, creating firewalls and access controls so that if one area of Equifax's information systems is compromised, hackers cannot gain access to other portions of Equifax's systems; (5) ordering that Equifax purge, delete, and destroy in a reasonably secure manner Class members' data not necessary for its provisions of services; (6) ordering that Equifax conduct regular database scanning and security checks; and (7) 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.

SIXTH CAUSE OF ACTION

Violation of the Ohio Data Breach Notification Statute
(R.C. § 1349.19)
(On Behalf of the Ohio Subclass only)

87. Plaintiff Benjamin Katz incorporates and re-alleges all allegations contained in the preceding and subsequent paragraphs as if fully set forth herein. Plaintiff and the other members of the Ohio Subclass are Class members whose Personal Information Equifax used for personal and private use.

88. The breach revealed by Equifax on September 7, 2017 was a data breach whereby the Personal Information of members of the Class and Subclasses, including the Ohio Subclass, was acquired or accessed in a way that compromised its security and confidentiality.

Accordingly, Equifax was required by law to notify the affected individuals in the most expedient time and manner possible and without unreasonable delay.

89. By failing to timely and expediently notify the Ohio Subclass of the data breach, Equifax violated Ohio's R.C. § 1349.19, which provides, in part:

> (B) (1) Any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. . . .
>
> (2) The person shall make the disclosure described in division (B)(1) of this section in the most expedient time possible but not later than forty-five days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described in division (D) of this section and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system.
>
> ***
>
> (D) The person may delay the disclosure or notification required by division (B), (C), or (G) of this section if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the person shall make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security.

90. The Breach constituted a "breach of the security of the system" of Equifax within the meaning of the above Ohio data breach notification statute in that there was an unauthorized access to and acquisition of computerized data that included Personal Information which was reasonably believed by all to have caused a material risk of identity theft or other fraud to residents of Ohio. The data breached was therefore protected and covered by the data breach notification statute.

91. Equifax unreasonably delayed informing the public, including Plaintiff Benjamin Katz and the members of the Ohio Subclass, about the data breach after Equifax knew or should have known that the data breach had occurred.

92. Equifax failed to disclose the Breach to Plaintiff Benjamin Katz and the other members of the Ohio Subclass without unreasonable delay and in the most expedient time possible.

93. Plaintiff Benjamin Katz and the other members of the Subclass suffered harm directly resulting from Equifax's failure to provide and the delay in providing notification of the Breach with timely and accurate notice as required by law.

94. As a result of said practices, Equifax has directly, foreseeably, and proximately caused damages to Plaintiff Benjamin Katz and the other members of the Ohio Subclass. Had Equifax provided timely, expedient, and accurate notice of the Breach, Plaintiff Benjamin Katz and the other members of the Ohio Subclass 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 Subclass members could have avoided providing further data to Equifax, could have avoided use of Equifax's services, and could otherwise have tried to avoid and monitor any harm caused by Equifax's delay in providing timely and accurate notice.

SEVENTH CAUSE OF ACTION

Violation of the New Jersey Data Notification Statute
(N.J.S.A. 56:8-163)
(On Behalf of the New Jersey Subclass only)

95. Plaintiff Josef Katz incorporates and re-alleges all allegations contained in the preceding and subsequent paragraphs as if fully set forth herein. Plaintiff and the other members

of the New Jersey Subclass are Class members whose Personal Information Equifax used for personal and private use.

96. By failing to timely notify the New Jersey Subclass of the data breach, Equifax violated N.J.S.A. 56:8-163, which provides, in part:

> a. Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.
>
> b. Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.
>
> c. (1) Any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.
>
> (2) The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.

97. The Breach constituted a "Breach of security" of Equifax within the meaning of the above New Jersey data breach statute and the data breached was protected and covered by the data breach statute.

98. Equifax unreasonably delayed informing the public, including Plaintiff and the members of the Subclass, about the data breach after Equifax knew or should have known that the data breach had occurred.

99. Equifax failed to disclose the Breach to Plaintiff Josef Katz and the other members of the New Jersey Subclass without unreasonable delay and in the most expedient time possible.

100. Plaintiff Josef Katz and the other members of the New Jersey Subclass suffered harm directly resulting from Equifax's failure to provide and the delay in providing notification of the Breach with timely and accurate notice as required by law.

64. As a result of said practices, Equifax has directly, foreseeably, and proximately caused damages to Plaintiff Josef Katz and the other members of the New Jersey Subclass. Had Equifax provided timely and accurate notice of the Breach, Plaintiff Josef Katz and the other members of the New Jersey Subclass 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 Josef Katz and the New Jersey Subclass members could have avoided providing further data to Equifax, could have avoided use of Equifax's services, and could otherwise have tried to avoid and monitor any harm caused by Equifax's delay in providing timely and accurate notice.

EIGHTH CAUSE OF ACTION

Violation of the New York Data Breach Notification Statute
(GBL § 899-aa)
(On Behalf of the New York Subclass only)

101. Plaintiff Leslie Katz incorporate and re-allege all allegations contained in the preceding and subsequent paragraphs as if fully set forth herein. Plaintiff Leslie Katz and the other members of the New York Subclass are Class members whose Personal Information Equifax used for personal and private use.

102. By failing to timely notify the New York Subclass of the data breach, Equifax violated GBL § 899-aa, which provides, in part:

> 2. Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
>
> * * *
>
> 4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.
>
> * * *
>
> 7. Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and

> private information were, or are reasonably believed to have been, so acquired.

103. Further, New York law provides that, "in addition to any other lawful remedy," "[w]henever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to ten dollars per instance of failed notification, provided that the latter amount shall not exceed one hundred fifty thousand dollars."

104. The Breach constituted a "[b]reach of the security of the system" of Equifax within the meaning of the above New York data breach statute and the data breached was protected and covered by the data breach statute.

105. Equifax unreasonably delayed informing the public, including Plaintiff Leslie Katz and the members of the New York Subclass, about the data breach after Equifax knew or should have known that the data breach had occurred.

106. Equifax failed to disclose the Breach reach to Plaintiff Leslie Katz and the other members of the New York Subclass without unreasonable delay and in the most expedient time possible.

107. Plaintiff Leslie Katz and the other members of the New York Subclass suffered harm directly resulting from Equifax's failure to provide and the delay in providing notification of the Breach with timely and accurate notice as required by law.

108. As a result of said practices, Equifax has directly, foreseeably, and proximately caused damages to Plaintiff Leslie Katz and the other members of the New York Subclass. Had Equifax provided timely and accurate notice of the Breach Plaintiff Leslie Katz and the other members of the New York Subclass 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 Leslie Katz and the New York Subclass members could have avoided providing further data to Equifax, could have avoided use of Equifax's services, and could otherwise have tried to avoid and monitor any harm caused by Equifax's delay in providing timely and accurate notice.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully request that this Court:

A. Certify this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), and appoint the Plaintiffs as Class and Subclass representatives and their counsel as Class Counsel;

B. Award Plaintiffs and the other members of the Class and Subclass appropriate relief, including actual and statutory damages;

C. Enter judgment in favor of Plaintiffs and the other members of the Class and against the Defendant under the legal theories alleged herein;

D. Award reasonable attorneys' fees, costs, and expenses;

E. Award the Plaintiffs and the other members of the Class and Subclass pre-judgment and post-judgment interest at the maximum rate allowable by law;

F. Award Plaintiffs and the other members of the Class and Subclass equitable, injunctive and declaratory relief as may be appropriate under applicable laws;

G. Enter Declaratory Judgment that the provisions in Equifax's Liability Limit and Choice of Law Provision do not constitute binding agreements and are unconscionable and unenforceable;

H. Enter such additional orders or judgment as may be necessary to prevent a recurrence of the Breach and to restore any interest or any money or property which may have been acquired by means of violations set forth in this Complaint; and

I. Grant such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

Dated: September 28, 2017

Respectfully submitted,

s/ David Worley
David Worley
Ga. Bar No. 776665
James M. Evangelista
Ga. Bar No. 070807
Kristi Stahnke McGregor
Ga. Bar No. 674012
EVANGELISTA WORLEY, LLC
8100A Roswell Road
Suite 100
Atlanta, GA 30350
404-205-8400
jim@ewlawllc.com
david@ewlawllc.com
kristi@ewlawllc.com

OF COUNSEL:

ABRAHAM, FRUCHTER & TWERSKY, LLP
Jeffrey S. Abraham
Matthew E. Guarnero
One Penn Plaza, Suite 2805
New York, New York 10119
Tel.: 212-279-5050
JAbraham@aftlaw.com
MGuarnero@aftlaw.com

Counsel for Plaintiffs

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)

LESLIE KATZ, BENJAMIN KATZ, and JOSEF KATZ, Individually and on Behalf of all Others Similarly Situated,

DEFENDANT(S)

EQUIFAX, INC.

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF New York County, NY
(EXCEPT IN U.S. PLAINTIFF CASES)

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT _____
(IN U.S. PLAINTIFF CASES ONLY)

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

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

James M. Evangelista, David J. Worley and Kristi Stahnke McGregor
EVANGELISTA WORLEY LLC
8100A Roswell Rd., Suite 100, Atlanta, GA 30350
Ph: (404)205-8400; jim@ewlawllc.com

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 pursuant to 28 U.S.C. § 1332(d)(2) whereby defendant, among other things, failed to adequately protect Plaintiffs' personal and credit data in violation of statutory and common law.

(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 _____ (Referral) NATURE OF SUIT _____ CAUSE OF ACTION _____

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 $ TBD

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.

David J. Worley By BK — 9/28/17

SIGNATURE OF ATTORNEY OF RECORD — DATE

Judge	Civil Action Number
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 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 Amy Totenberg	1:17-cv-03578
Judge Amy Totenberg	1:17-cv-03518