UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF GEORGIA

ATLANTA DIVISION

Carmen Pellitteri and Kent Toft, individually and on behalf of all others similarly situated, Plaintiffs v. Equifax, Inc., Defendant	CLASS ACTION COMPLAINT JURY TRIAL DEMANDED CIVIL ACTION NO: _____

Plaintiffs Carmen Pellitteri and Kent Toft, by and through their undersigned counsel, individually and on behalf of a class of all similarly situated individuals and entities in the United States, file this Class Action Complaint against Defendant Equifax, Inc. ("Equifax"), and state the following:

INTRODUCTION

1. This litigation is the result of one of the largest data breaches in history of the financial services industry, against one of the three major U.S. credit bureaus.

Credit bureaus perform one primary task: collecting and maintaining consumers' most sensitive personal and financial information.

2. One credit bureau—Equifax—completely failed this task. Their negligence allowed hackers to breach their website and gain unfettered access to the sensitive information of over a hundred million Americans. As a result, Equifax set off a chain reaction that threatens the trustworthiness and stability of the financial system for individuals and institutions alike.

3. Equifax is one of the largest consumer credit bureaus in the United States. Equifax gathers, analyzes, and maintains credit-reporting information on over 820 million individual consumers and over 91 million businesses.

4. On September 7, 2017, Equifax announced that hackers had exploited a vulnerability in Equifax's U.S. website to illegally gain access to consumer files.[1]

5. Equifax must be held accountable for its failures and for a cybersecurity breach so massive that it could prove detrimental to the health of the American economy and to tens of millions of American consumers.

6. Plaintiffs file this complaint as a national class action on behalf of over 140 million consumers across the country harmed by Equifax's failure to adequately

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

protect their credit and sensitive personal information. This complaint requests Equifax provide fair compensation in an amount that will ensure every consumer harmed by Equifax's data breach will not be out-of-pocket for the costs of independent third-party credit repair and monitoring services. This complaint's allegations are based on personal knowledge as to Plaintiffs' conduct and made on information and belief as to the acts of others.

THE PARTIES

7. Plaintiff Carmen Pellitteri is an individual consumer residing in the Lantana, Florida area.

8. Plaintiff Kent Toft is an individual consumer residing in the Blaine, Minnesota area.

9. Defendant Equifax Inc. (Equifax) is a Georgia corporation that maintains its principal place of business at 1550 Peachtree Street NE, Atlanta, Georgia. Equifax operates through various subsidiaries, including Equifax Information Services, LLC, and Equifax Consumer Services, LLC, aka Equifax Personal Solutions, aka PSOL. Each of these entities acted as agents of Equifax, or in the alternative, acted in concert with Equifax as alleged in this complaint.

JURISDICTION AND VENUE

10. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because (1) the Class consists of more than 100 members; (2) the amount at issue is more than $5 million exclusive of interest and costs; and (3) minimal diversity exists as at least one plaintiff is a citizen of a different state than Defendant.

11. This Court has jurisdiction over Equifax because the company maintains its principal headquarters in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts with Georgia. Equifax intentionally avails itself of this jurisdiction by marketing and selling products from Georgia to millions of consumers nationwide (including in Georgia).

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

FACTUAL ALLEGATIONS

13. Equifax is one of the largest consumer credit reporting agencies in the United States, and it is the oldest of the three major U.S. credit-reporting agencies.

Equifax has over $3 billion in annual revenue, and its common stock is traded on the New York Stock Exchange.

14. Equifax gathers and maintains credit-reporting information on over 820 million individual consumers and over 91 million businesses.

15. For consumer files, Equifax collects a substantial amount of sensitive personal information. Equifax's consumer credit files include individuals' names, current and past addresses, birth dates, social security numbers, driver's license information, and telephone numbers; credit account information, including the institution name, type of account, date the account was opened, payment history, credit limit, and balance; credit inquiry information, including credit applications; and public-record information, including liens, judgments, and bankruptcy filings.

16. Throughout the past year, Equifax collected and stored sensitive personal and financial information about Mr. Pellitteri and Mr. Toft.

17. Equifax analyzes the information that it collects and generates consumer credit reports, which it sells to businesses like retailers, insurance companies, utility companies, banks and financial institutions, and government agencies.

18. Equifax also provides services 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 to consumers to use every reasonable measure to protect the sensitive consumer information that it collects from exposure to hackers and identity thieves.

The Equifax Data Breach

20. Equifax reported that from mid-May to late July of 2017, hackers exploited a vulnerability in Equifax's U.S. web server software to illegally gain access to certain consumer files. Investigators believe that the point of entry may have been a software application called Apache Struts.[2]

21. 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. Despite this warning, Equifax continued to use the software. And Equifax was reportedly using an outdated version of Apache Struts at the time of the data breach.[3]

[2] AnnaMaria Androtis *et al., Equifax Hack Leaves Consumers, Financial Firms Scrambling*, WALL STREET JOURNAL, Sept. 8, 2017, *available at* https://www.wsj.com/articles/equifax-hack-leaves-consumers-financialfirms-scrambling-1504906993.
[3] *Id.*

22. Although Equifax claims the breach began in May, reports from a noted computer security firm, FireEye, Inc., indicated that the breach likely started as early as March 10.[4] Equifax has claimed that this March breach was unrelated to the current breach, although some believe that it was the same group of hackers.[5]

23. Over this lengthy period, the Equifax hackers accessed consumer names, social security numbers, birth dates, addresses, and driver's license numbers.[6] The compromised data contains complete profiles of consumers whose personal information was collected and maintained by Equifax. In fact, it is likely that the extended time of the breach allowed the hackers to "escalate their privileges and intrude further into the Equifax network" and enter the same database commands as "high-privilege Equifax administrators."[7]

24. Equifax estimates that 143 million Americans were impacted by this breach, although it admits that it is still in the process of "conducting a

[4] Ars Technica, *Massive Equifax Hack Reportedly Started 4 Months Before It Was Detected* (Sept. 20, 2017) , available at https://arstechnica.com/information-technology/2017/09/massive-equifax-hack-reportedly-started-4-months-before-it-was-detected/. *See also* AnnaMaria Androitis, *et al.*, *Hackers Entered Equifax Systems in March*, WALL STREET JOURNAL Sept. 20, 2017, available at https://www.wsj.com/articles/hackers-entered-equifax-systems-in-march-1505943617.
[5] Michael Riley, *et al.*, *Equifax Suffered A Hack Almost Five Months Earlier Than The Date It Disclosed*, BLOOMBERG TECHNOLOGY (Sept. 18, 2017), available at https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed.
[6] *Id.*
[7] *Id.*

comprehensive forensic review" with a cybersecurity firm "to determine the scope of the intrusion."[8]

25. In addition to accessing sensitive personal information, the hackers also accessed an estimated 209,000 consumer credit card numbers, and an estimated 182,000 dispute records containing additional personal information were compromised.[9]

26. Equifax reportedly discovered this breach on July 29, 2017.[10]

27. After Equifax discovered this breach but before Equifax disclosed the breach to the public, three high-level executives sold shares in the company worth nearly $1.8 million.[11] 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.

28. Equifax did not report this breach to the public until September 7, 2017 – almost six weeks after it had reportedly discovered the breach. Equifax has not

[8] Equifax, *Cybersecurity Incident & Important Consumer Information* (Sept. 8, 2017), available at https://www.equifaxsecurity2017.com/.
[9] *Id.*
[10] *Id.*
[11] Anders Melin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed*, BLOOMBERG (Sept. 7, 2017), available at https://www.bloomberg.com/news/articles/2017-09-07/three-equifaxexecutives-sold-stock-before-revealing-cyber-hack.

explained its delay in reporting this breach to the public. The FBI and federal regulators are investigating the breach, and two congressional committees announced that they would hold hearings.[12]

29. Upon information and belief, although weeks have passed since Equifax discovered the breach, the federal investigations are still ongoing, and the identities of the hackers are still unknown.

30. 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."[13]

31. The Equifax breach is unique because many consumers may not be aware that their personal information was compromised. Equifax obtains its credit reporting information from banks, credit card issuers, retailers, lenders, and public records. Accordingly, many consumers are not aware that Equifax or other reporting companies are collecting or retaining their sensitive personal information.

[12] Androtis, *Equifax Hack, supra*.
[13] *Id.*

Consumers Are Harmed by the Breach

32. Initial reports indicate that hackers accessed the sensitive personal and financial information of approximately 143 million U.S. consumers in this breach.

33. Identity thieves can use information such as credit card numbers to make fake credit cards, which can then be sold or used to make unauthorized purchases that are then charged to a customer's account.

34. Additionally, 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 then use these data sets 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 customer's name, obtain government benefits, or file a fraudulent tax return.

35. When identity thieves fraudulently use a victim's personal information, the victim frequently suffers financial consequences. A 2014 Department of Justice

report on identity theft reported that 65% of identity theft victims experienced direct or indirect financial losses.

36. When sensitive personal information is compromised, consumers must exercise constant vigilance on their financial and personal records to ensure that fraudulent activity has not occurred. Consumers are forced to spend additional time monitoring their credit and finances as well as dealing with any potentially fraudulent activity.

37. Consumers also face significant emotional distress after theft of their identity. The fear of financial harm can cause significant stress and anxiety for many consumers. According to the Department of Justice, an estimated 36% of identity theft victims experienced moderate or severe emotional distress as a result of the crime.[14]

38. Equifax had a duty to properly secure its 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 Plaintiffs and the Class, which it knew would result from a data breach.

[14] *Id.*

The Breach was Enabled by Equifax's Failure to Adequately and Properly Secure its U.S. Website

39. The Equifax breach was the direct result of Equifax's failure to properly and adequately secure its U.S. website.

40. 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.

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

42. Equifax should have recognized and identified the flaws in its data security and should have taken measures to fix these vulnerabilities. Equifax had a duty to take advantage of what experts had already learned about security vulnerabilities and to use industry best practices, such as updating software to the latest version, to prevent a security breach.

43. 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.[15] Equifax had a duty to respond to a report of a significant software security flaw. Despite Equifax's knowledge of these potential security threats, Equifax willfully (or at the very 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.

44. The harm to consumers and financial institutions as a result of Equifax's failure to adequately secure its computer systems and websites was therefore foreseeable to Equifax.

45. Equifax is well aware of the costs and risks associated with identity theft. On its website, Equifax lists "some of the ways identity theft might happen," including when identity thieves "steal electronic records through a data breach."

[15] Androtis, *Equifax Hack, supra*. *See also*, Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES, Sept. 8, 2017, available at https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-databreach-history/#63dc4270677c.

How Does Identity Theft Happen?

Identity thieves have gotten more sophisticated in their methods. The following includes some of the ways identity theft may happen:

- Steal wallets or purses in order to obtain identification, credit and bank cards;
- Dig through mail and trash in search of bank and credit card statements, preapproved credit card offers, tax information and other documents that may contain personal details;
- Fill out change-of-address forms to forward mail, which generally contains personal and financial information;
- Buy personal information from an inside, third party source, such as a company employee who has access to applications for credit;
- Obtain personnel records from a victim's place of employment;
- "Skim" information from an ATM — this is done through an electronic device, which is attached to the ATM, that can steal the information stored on a credit or debit card's magnetic strip;
- Swipe personal information that has been shared on unsecured websites or public Wi-Fi;
- Steal electronic records through a data breach;
- "Phish" for electronic information with phony emails, text messages and websites that are solely designed to steal sensitive information;
- Pose as a home buyer during open houses in order to gain access to sensitive information casually stored in unlocked drawers.

16

46. In fact, Equifax has published a report on the "Emotional Toll of Identity Theft." In its report, Equifax states that "identity theft victims may experience similar emotional effects as victims of violent crimes, ranging from anxiety to emotional volatility." The report also cites a survey finding that "69 percent felt fear for personal financial security; 50 percent of respondents said they had feelings of powerlessness or helplessness; and 29 percent said they felt shame or embarrassment."[17]

47. Because Equifax is aware of the negative consequences of identity theft, Equifax also offers products aimed at protecting consumers from identity theft.

[16] Equifax, *How Does Identity Theft Happen?*, available at https://www.equifax.com/personal/education/identity-theft/how-doesidentity-theft-happen (last visited September 20, 2017).

[17] Equifax, *A Lasting Impact: The Emotional Toll of Identity Theft*, Feb. 2015, available at https://www.equifax.com/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf.

For example, Equifax advertises its "Equifax Complete™ Premier Plan" as "Our Most Comprehensive Credit Monitoring and Identity Protection Product."[18] The product promises to alert consumers of changes to their credit score and credit report, provide text message alerts to changes, lock the consumer's credit file to protect against unapproved third parties, and automatically scan suspicious websites for consumers' personal information.

48. 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—including Plaintiffs and the other class members.

Equifax Had a Duty to Prevent and Timely Report this Breach

49. Equifax had a duty to prevent breach of consumers' sensitive personal information.

50. Following several high-profile data breaches in recent years, including Target, Home Depot, Yahoo, and Sony, 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. Nonetheless,

[18] Equifax, *Equifax Complete ™ Premier Plan: Our Most Comprehensive Credit Monitoring and Identity Protection Product*, available at https://www.equifax.com/personal/products/credit/monitoring-and-reports (last visited Sept. 20, 2017).

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

51. Consumers and financial institutions were harmed not only by the breach itself but also by Equifax's failure to timely report this breach to the public. 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.

52. According to the Wall Street Journal, 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."[19] 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 were able to sell—and sold—substantial sums of stock in the company, presumably avoiding the financial losses associated with the negative press Equifax has received since the breach.[20]

[19] Androtis, *Equifax Hack, supra*.

[20] 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), available at https://blogs.wsj.com/moneybeat/2017/09/08/equifaxshares-on-pace-for-worst-day-in-18-years/.

53. 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.

54. Financial institutions have also 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.

55. This resulted in additional harm to Plaintiff, the Class, and consumers that they would not have suffered if Equifax had not delayed in reporting the breach to the public.

CLASS ALLEGATIONS

56. Plaintiffs bring this action on behalf of themselves and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), on behalf of the following class:

> Consumers in the United States (including its Territories and the District of Columbia) whose personal information was collected or amassed by Equifax and compromised in the 2017 breach of Equifax's U.S. website (the "Class").

57. Excluded from the class are all attorneys for the class, officers and members of Equifax, including officers and members of any entity with an

ownership interest in Equifax, the Court and its employees, officers, and relatives, and all jurors and alternate jurors who sit on the case.

58. Plaintiffs are members of the Class, as defined above.

59. The members of the Class are readily ascertainable, and Equifax likely has access to addresses and other contact information that may be used for providing notice to Class members.

60. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used in individual actions alleging the same claims.

61. This action has been brought and may be properly maintained on behalf of the class proposed herein under Federal Rule of Civil Procedure 23 and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of its provisions.

62. **Numerosity** - The class is so numerous that joinder is impracticable. Upon information and belief, and based upon Equifax's own estimate, this data breach has affected approximately 143 million consumers nationwide.

63. **Commonality** - Common questions of fact and law predominate over any questions affecting only individual class members. Common questions include

whether Plaintiffs and the class members are entitled to equitable relief, whether Equifax acted negligently, and whether Plaintiffs and the class members are entitled to recover money damages. Common factual and legal questions include, but are not limited to:

a. whether Equifax failed to provide adequate security and/or protection on its websites that contained sensitive consumer information;

b. whether Equifax's conduct resulted in the breach of its U.S. website and the exposure of consumers' sensitive information;

c. whether Equifax notified the public of this breach in a timely manner;

d. whether Equifax failed to encrypt sensitive consumer information;

e. whether Equifax's actions were negligent;

f. whether Equifax owed a duty to Plaintiffs and the Class;

g. whether the harm to Plaintiffs and the Class was foreseeable;

h. whether Plaintiffs and the Class are entitled to injunctive relief; and

i. whether Plaintiffs and the Class are entitled to damages, and the amount of such damages.

64. **Typicality** - Plaintiffs' claims are typical of the claims of the class because each suffered risk of loss and credit harm and identity theft caused by

Equifax's negligent failure to safeguard their data, many of the injuries suffered by Plaintiffs and the class members are identical (i.e. the costs to monitor and repair their credit through a third-party service for at least 24 months), and Plaintiffs' claims for relief are based upon the same legal theories as are the claims of the other class members.

65. **Adequacy** - Plaintiffs will fairly and adequately protect and represent the interests of the class because their interests do not conflict with the interests of the class they seek to represent, they are represented by counsel who are qualified and competent and have significant experience handling complex class action litigation and consumer protection cases, and who will vigorously prosecute this litigation. Plaintiffs and their counsel will fairly and adequately protect the class's interests in this case.

66. **Superiority** – A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the other Class members' claims is economically unfeasible and procedurally impracticable. Litigating the claims of the Class together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and unnecessary expense to the parties and the courts.

CAUSES OF ACTION

Count 1
NEGLIGENCE

67. Plaintiffs incorporate by reference all preceding allegations as though fully set forth herein.

68. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care and diligence in obtaining, processing, and retaining Plaintiffs' sensitive personal information and credit card numbers.

69. Defendant owed a duty to Plaintiffs and the Class to adequately secure consumers' personal and financial information.

70. Defendant breached this duty by: (1) failing to properly secure its U.S. website from intrusion by a third party; (2) allowing a third party to exploit a vulnerability in this website and access consumers' sensitive personal and financial information; (3) failing to detect this breach for several weeks; and (4) failing to notify consumers of this breach for nearly six weeks.

71. Defendant knew or should have known of the risks associated with potential vulnerabilities in its websites and computer systems.

72. Defendant knew or should have known that its failure to take reasonable measures to secure these websites and computer systems against obvious risks would result in harm to Plaintiffs and the Class.

73. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

Count II
NEGLIGENCE BY MISREPRESENTATION

74. Plaintiffs incorporate by reference all preceding allegations as though fully set forth herein.

75. Through collecting, analyzing, and maintaining sensitive consumer information, Equifax represented to Plaintiffs and the Class that it maintained adequate data security measures, and that the data security measures it employed were adequate to protect the sensitive consumer financial information maintained in its computer system.

76. Defendant knew or should have known that its data security measures were not, in fact, adequate to protect the sensitive consumer financial information maintained in its computer system.

77. Defendant failed to disclose vulnerabilities in its website and computer system that made its sensitive consumer information susceptible to breach.

78. Defendant was required to disclose this fact to Plaintiffs, the Class, and consumers.

79. Defendant also failed to timely discover the breach, and failed to timely disclose the breach to Plaintiffs, the Class, and consumers once Defendant had discovered it.

80. Had Plaintiffs, the Class, and consumers been aware of the vulnerabilities in Defendant's websites and computer systems, leaving sensitive consumer information susceptible to breach, Plaintiffs, the Class, and consumers would have taken action to prevent this data from being breached or required Equifax to take immediate action to resolve these weaknesses.

81. As a direct and proximate result of Defendant's negligent misrepresentation by omission, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

Count III
DECLARATORY AND INJUNCTIVE RELIEF

82. Plaintiffs incorporate by reference all preceding allegations as though fully set forth herein.

83. Plaintiffs and the Class are entitled to a declaratory judgment under the Declaratory Judgment Act, 28 U.S.C. § 2201 et seq. The Declaratory Judgment Act authorizes this Court to enter a declaratory judgment stating the rights and legal relations of the parties and grant further relief if necessary. Additionally, the Court has authority to enjoin tortious acts or acts in violation of federal or state statute.

84. Plaintiffs and the Class contend that Equifax's data security measures were inadequate to protect consumers' sensitive personal information. Upon information and belief, these data security measures remain inadequate. Plaintiffs and the Class will continue to suffer injury unless this is rectified.

85. Plaintiffs and the Class seek a declaratory judgment stating that Equifax owed and continues to owe a duty to adequately and appropriately secure consumers' sensitive personal and financial information, and that Equifax has a duty to timely disclose to the public any breach of that data; that Equifax breached and continues to breach this duty by failing to adequately secure its websites and computer systems containing members' or customers' sensitive personal and financial information; Equifax's breach of this duty caused the data breach which occurred between mid-May and late-June of 2017; and Plaintiffs and the Class have suffered damages as a result.

86. Plaintiff and the Class also seek corresponding injunctive relief requiring Equifax to use adequate security measures to protect its websites and computer systems from attacks by hackers and to prevent future unauthorized access of consumers' sensitive personal and financial information.

87. If injunctive relief is not granted, Plaintiffs and the Class will suffer irreparable injury and will not have an adequate legal remedy in the event of future

data breaches. Many of the injuries resulting from these breaches are not easily quantifiable, and Plaintiffs and the Class will be forced to bring multiple additional lawsuits.

88. The burden to Equifax if this Court issues an injunction is far greater than the burden to Plaintiffs and the Class if the Court does not do so. The cost of improving data security and applying reasonable measures to protect consumer data should be minimal, particularly given the nature of Equifax's business and its considerable financial resources. Equifax already has a duty to provide these protections. If future data breaches occur, though, upon information and belief, Plaintiffs and the Class will suffer further damages.

89. Such an injunction would benefit the public by decreasing the risk of future Equifax data breaches, eliminating potential future injuries that would result from another breach.

90. Plaintiffs and Class members, therefore, request the injunctive and declaratory relief detailed above.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of themselves and the Class, respectfully request that the Court enter judgment in their favor as follows:

a. Certifying the Class under Fed. R. Civ. P. 23 and appointing Plaintiffs and their counsel to represent the Class pursuant to Fed. R. Civ. P. 23(g);

b. An order temporarily and permanently enjoining Equifax from the negligent business practices alleged in this Complaint;

c. Awarding Plaintiffs and the Class monetary damages as allowable by law;

d. Awarding Plaintiffs and the Class appropriate equitable relief;

e. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest;

f. Awarding Plaintiffs and the Class reasonable attorneys' fees and costs as allowable by law; and

g. Awarding all such further relief as allowable by law.

JURY TRIAL DEMANDED

Plaintiffs, on behalf of themselves and the Class, demand a trial by jury on all issues so triable.

Respectfully submitted this 4th day of October, 2017.

/s/ David A. Bain
David A. Bain
LAW OFFICES OF DAVID A. BAIN, LLC
Georgia Bar No. 032449
1230 Peachtree Street N.E.
Suite 1050
Atlanta, GA 30309
Telephone: (404) 724-9990
Facsimile: (404) 724-9986
dbain@bain-law.com

REINHARDT WENDORF & BLANCHFIELD
Mark Reinhardt
Garrett D. Blanchfield
Brant D. Penney
Roberta A. Yard
E-1250 First National Bank Building
332 Minnesota Street
St. Paul, MN 55101
Telephone: (651) 287-2100
m.reinhardt@rwblawfirm.com
g.blanchfield@rwblawfirm.com
b.penney@rwblawfirm.com
r.yard@rwblawfirm.com

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)

Carmen Pellitteri and Kent Toft, individually and on behalf of all others similarly situated,

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Palm Beach County, FL
(EXCEPT IN U.S. PLAINTIFF CASES)

DEFENDANT(S)

Equifax, Inc.

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)

Law Offices of David A. Bain, LLC
1230 Peachtree St., NE, Suite 1050
Atlanta, GA 30309
404-724-9990
dbain@bain-law.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)

Consumer class action asserting violations of state law, seeking legal and equitable relief in connection with a data 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 _____ (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 $_____

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

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE Duffey DOCKET NO. 1:17-CV-3422-WSD

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 A. Bi 10/4/17

SIGNATURE OF ATTORNEY OF RECORD DATE