

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA**

KIRBY WILKINS, Individually and On
Behalf of All Others Similarly Situated,

Plaintiff,

v.

EQUIFAX, INC.,

Defendant.

Civil Action No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

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

NATURE OF THE ACTION

1. This is a class action on behalf of the 143 million individuals whose sensitive personal identifying information was compromised in a cybersecurity breach of Equifax, which was announced on September 7, 2017 (the “Equifax Breach”).

2. According to Company’s public announcement of the Equifax Breach, the compromised information includes Social Security numbers, birth dates,

addresses and, in some instances, driver's license numbers. Also, hackers accessed credit card numbers and certain dispute documents with personal identifying information for some consumers.

3. Equifax failed to adequately protect consumers' sensitive personal identifying information. Lack of proper safeguards provided a means for unauthorized intruders to breach Equifax's computer network and steal sensitive personal identifying information.

4. Armed with this sensitive personal identifying information, hackers can commit a variety of crimes including, among other things, taking out loans in another person's name; opening new financial accounts in another person's name; using the victim's information to obtain government benefits; filing a fraudulent tax return and using the victim's information to obtain a tax refund; obtaining a driver's license or identification card in the victim's name but with another person's picture; or giving false information to police during an arrest.

5. As a result of the Equifax Breach, Plaintiff and Class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class members must now and in the future closely monitor their financial accounts to guard against identity theft. Plaintiff and Class members may be faced with fraudulently incurred debt. Plaintiff and Class members may also

incur out of pocket costs for, among other things, obtaining credit reports, credit freezes, or other protective measures to deter or detect identity theft.

6. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly-situated individuals and entities whose sensitive personal identifying information was accessed during the Equifax Breach.

7. Plaintiff seeks remedies including but not limited to reimbursement of out-of-pocket losses, further credit monitoring services with accompanying identity theft insurance, and improved data security.

PARTIES

8. Plaintiff Kirby Wilkins resides and is a citizen of the state of Georgia.

9. In response to Company's announcement of the Equifax Breach, Plaintiff visited the Equifax Breach Website (defined below) and confirmed that her sensitive personal identifying information had been compromised by the Equifax Breach.

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

11. Equifax describes itself as a "global information solutions company." The company organizes, assimilates and analyzes data on more than 820 million

consumers ...” and among Equifax’s business lines are “consumer and commercial credit reporting and scoring.”¹

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). If a class is certified in this action, the amount in controversy will exceed \$5,000,000.00, exclusive of interest and costs. At least one member of the proposed class is a citizen of a state different from Equifax. Greater than two-thirds of the members of the proposed class are citizens of states other than Georgia.

13. This Court has personal jurisdiction over Equifax, because Equifax is incorporated in, and its headquarters and principal place of business are located within, Georgia.

14. Venue is also proper within this District because, pursuant to 28 U.S.C. § 1391(b)(1) & (c)(1), Equifax is deemed to reside in this District since it is subject to personal jurisdiction in this District. Finally, venue is proper in this District because a substantial part of the events or omissions giving rise to the claim occurred in this District.

¹<https://investor.equifax.com/~media/Files/E/Equifax-IR/Annual%20Reports/2016-annual-report.pdf>

SUBSTANTIVE ALLEGATIONS

THE EQUIFAX BREACH

15. According to a statement released by Equifax on September 7, 2017:

Equifax, Inc. [] today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers... 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.²

16. Equifax briefly explained that, “[c]riminals exploited a U.S. website application vulnerability to gain access to certain files.” Equifax also disclosed that “unauthorized access occurred from mid-May through July 2017.”³

17. According to Equifax, its “Security team observed suspicious network traffic associated with its U.S. online dispute portal web application” on July 29, 2017, which is when the Company purportedly first discovered the Equifax Breach.⁴

18. The Company, however, delayed its public announcement of Equifax Breach until September 7, 2017.⁵

² <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>

³ *Id.*

⁴ *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, EQUIFAX (Sept. 15, 2017), <https://www.equifaxsecurity2017.com/>.

⁵ <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>

19. In describing the breach, Equifax’s Chairman and Chief Executive Office, Richard F. Smith, released the following statement:

This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. 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.⁶

20. On September 15, 2017, the Company revealed that the Equifax Breach was the result of a vulnerability in Apache Struts (CVE-2017-5638)—an open-source application framework that supports Equifax’s online dispute portal application. This vulnerability was first disclosed in the United States in early March 2017, and Equifax’s security team had unsuccessfully attempted to patch “any vulnerable systems in the company’s IT infrastructure.”⁷

21. Further, the Equifax Breach was not the first time the Company was the subject of a cybersecurity breach. Equifax previously suffered a breach in March of 2017 – just a few months prior to the Equifax Breach. It has been

⁶ *Id.*

⁷ *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, EQUIFAX (Sept. 15, 2017), <https://www.equifaxsecurity2017.com/>.

reported that the prior breach and the Equifax Breach were perpetrated by the same hackers.⁸

22. Despite this prior breach, Equifax failed to adopt adequate protective measures to prevent the exploitation of a vulnerability in a website application and failed to ensure that consumers' sensitive personal identifying information would not be improperly accessed.

23. Once Equifax's systems had been compromised, Equifax failed to timely discover the breach and implement adequate remedial measures to secure consumers' sensitive personal identifying information.

24. As a result of Equifax's inadequate measures, sensitive personal identifying information was obtained from Equifax's computer network over a period of approximately six weeks before detection.

25. Moreover, Equifax failed to timely inform consumers of the Equifax Breach – waiting over a month after it was discovered before making its public announcement.

EQUIFAX'S POST-BREACH ACTIONS ARE INADEQUATE

26. In the wake of the Equifax Breach, the Company has established a dedicated website, <https://www.equifaxsecurity2017.com/> (the "Equifax Breach Website"), which allows consumers to determine if they were impacted by the

⁸ *Id.*

breach. The website also allows affected consumers to sign up for credit monitoring and theft protection through TrustedID Premier, however the enrollment period for such services ends on January 31, 2018.⁹

27. There have been reports that the Equifax Breach Website has not functioned for potentially affected consumers.¹⁰ And, it has also been reported that Equifax's credit monitoring website – which can be used by consumers to set up alerts regarding credit rating history may be vulnerable to additional hacking.¹¹

28. The Company has taken no steps to date to notify consumers of the Equifax Breach and the potential theft of their sensitive personal identifying information, aside from issuing its press release and establishing the Equifax Breach Website.¹²

29. Equifax claims that it will send direct mail notices of the breach to those consumers whose credit card numbers or dispute documents with personal identifying information have been stolen. Equifax, however, has no plans to independently notify the consumers whose sensitive personal identifying

⁹ <https://www.equifaxsecurity2017.com/enroll/>

¹⁰ See, e.g., <http://www.businessinsider.com/equifax-data-breach-site-check-angry-response-2017-9>; <http://www.marketwatch.com/story/after-huge-data-breach-equifax-not-telling-all-customers-if-they-are-affected-2017-09-07>

¹¹ <http://www.zdnet.com/article/equifax-freeze-your-account-site-is-also-vulnerable-to-hacking/>

¹² <https://www.equifaxsecurity2017.com/frequently-asked-questions/>

information – names, Social Security numbers, birth dates, addresses and driver’s license numbers – was compromised.¹³

30. Even consumers who are aware of the Equifax Breach, have been unable to secure immediate protections for their stolen data.

31. For example, consumers have reported delays and technical problems with Equifax, preventing them from obtaining credit freezes in the wake of the Equifax Breach.¹⁴

32. Moreover, even before it starts, Equifax has recognized the limitations in the credit monitoring and identity theft protection being offered to consumers.

33. For example, with respect to “Social Security Number Monitoring,” Equifax admits that “there is no guarantee that Identity Protection provided by Equifax is able to locate and search every possible internet site where consumers’ personal information is at risk of being traded.”¹⁵

34. With respect to identity theft insurance, Equifax recognizes that “[c]overage may not be available in all jurisdictions.”¹⁶

¹³<https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>

¹⁴https://mobile.nytimes.com/2017/09/14/your-money/equifax-answers-data-breach.html?em_pos=small&emc=edit_dk_20170915&nl=dealbook&nl_art=0&nli d=3681798&ref=headline&te=1&referer=

¹⁵ <https://www.equifaxsecurity2017.com/trustedid-premier/>

¹⁶ *Id.*

35. Further, the Terms of Use for TrustedID Premier – the Equifax entity through which Equifax is offering credit monitoring and identity theft protection – include arbitration and class action waiver clauses.¹⁷

36. Also notable, Equifax’s general Terms of Use state: “[w]e do not offer, provide, or furnish any Products, or any advice, counseling, or assistance, for the express or implied purpose of improving Your credit record, credit history, or credit rating.”¹⁸

37. The Data Breach Website has been criticized by Attorneys General throughout the United States, including Georgia Attorney General Christopher M. Carr.

38. On September 15, 2017, Attorney General Carr, along with thirty-two other Attorneys General, wrote to Equifax, stating, *inter alia*:

We are writing to raise our profound concerns regarding the massive data breach Equifax Inc. (“Equifax”) recently disclosed to the public. Early indications are the breach was caused by Equifax’s failure to apply a necessary patch to its software. The breach has exposed the personal information of as many as half the consumers residing in the United States and its territories. ***Our concerns have only been heightened by Equifax’s conduct since its disclosure of the breach. The webpage Equifax has dedicated to alerting the 143 million consumers potentially affected by the breach is causing a great deal of confusion and concern. Chief among the issues causing confusion and concern are the inclusion of terms of service that required consumers to waive their rights, the offer of competing fee-***

¹⁷ <https://www.trustedid.com/serviceterms.php>

¹⁸ <http://www.equifax.com/terms/>

*based and free credit monitoring services by Equifax, and the charges consumers incur for a security freeze with other credit monitoring companies like Experian, TransUnion, and Innovis.*¹⁹

39. The Attorneys General “object[ed] to Equifax seemingly using its own data breach as an opportunity to sell services to breach victims” and informed Equifax that “[s]elling a fee-based product that competes with Equifax’s own free offer of credit monitoring services to victims of Equifax’s own data breach is unfair, particularly if consumers are not sure if their information was compromised.”²⁰

40. The Consumer Financial Protection Bureau, the Federal Trade Commission and at least 34 state attorney generals have opened inquiries into the Equifax Breach.²¹

41. It has also been reported that three Equifax executives sold nearly \$2 million in shares in the company, days after the Equifax Breach was discovered

¹⁹https://law.georgia.gov/sites/law.georgia.gov/files/related_files/press_release/Equifax.Letter%20to%20Counsel.9-15-17.pdf (emphasis added).

²⁰ *Id.*

²¹<https://www.nytimes.com/2017/09/18/business/equifax-breach-federal-investigation.html>.

(but before it was announced publicly).²² The U.S. Department of Justice has reportedly opened a criminal investigation into the stock sales.²³

42. Further in the wake of the Equifax Breach, the Company's Chief Information Officer, Chief Security Officer and Chief Executive Officer have retired.²⁴

CLASS ACTION ALLEGATIONS

43. Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23 on behalf of the following class and sub-class:

All individuals and entities in the United States whose personal identifying information was accessed in the cybersecurity breach announced by Equifax on September 7, 2017 (the "Nationwide Class"); and

All individuals and entities in Georgia whose personal identifying information was accessed in the cybersecurity breach announced by Equifax on September 7, 2017 (the "Georgia Sub-Class").

44. Excluded from the Nationwide Class and Georgia Sub-Class are Equifax; any parent, subsidiary, or affiliate of Equifax or any employees, officers,

²²<https://www.cnn.com/2017/09/07/credit-reporting-firm-equifax-says-cybersecurity-incident-could-potentially-affect-143-million-us-consumers.html>

²³https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed?utm_campaign=news&utm_medium=bd&utm_source=applenews

²⁴*Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, EQUIFAX (Sept. 15, 2017), <https://www.equifaxsecurity2017.com/>; <https://finance.yahoo.com/news/equifax-shares-halted-news-pending-124726108.html>

or directors of Equifax; legal representatives, successors, or assigns of Equifax; and any justice, judge, or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

45. Upon information and belief, the Nationwide Class and Georgia Sub-Class consist of millions of geographically dispersed members, the joinder of whom in one action is impracticable. Disposition of the claims in a class action will provide substantial benefits to both the parties and the Court.

46. The rights of each member of the Nationwide Class and Georgia Sub-Class were violated in a similar fashion based upon Equifax's uniform wrongful actions and/or inaction.

47. The following questions of law and fact are common to each Class member and predominate over questions that may affect individual Class members:

- A. whether Equifax engaged in the wrongful conduct alleged herein;
- B. whether Equifax was negligent in collecting, storing, and/or safeguarding the sensitive personal identifying information of the Class members;

- C. whether Equifax owed a duty to Plaintiff and Class members to adequately protect their personal information;
- D. whether Equifax breached its duties to protect the personal information of Plaintiff and Class members;
- E. whether Equifax knew or should have known that its data security systems and processes were vulnerable to attack;
- F. whether Equifax's conduct proximately caused damages to Plaintiff and Class members;
- G. whether Equifax's conduct violated the Ga. Code Ann. § 10-1-912.
- H. whether Plaintiff and Class members are entitled to equitable relief including injunctive relief; and
- I. whether the Class members are entitled to compensation, monetary damages, and/or any other services or corrective measures from Equifax, and, if so, the nature and amount of any such relief.

48. Plaintiff's claims are typical of the claims of the Nationwide Class and Georgia Sub-Class in that Plaintiff, like all Class members, had her sensitive personal identifying information compromised in the Equifax Breach.

49. Plaintiff is committed to the vigorous prosecution of this action and will fairly and adequately represent and protect the interests of the proposed the Nationwide Class and Georgia Sub-Class. Plaintiff has no interests that are antagonistic to and/or that conflict with the interests of other putative Class members.

50. Plaintiff has retained counsel competent and experienced in the prosecution of complex class action litigation.

51. The members of the proposed the Nationwide Class and Georgia Sub-Class are readily ascertainable.

52. A class action is superior to all other available methods for the fair and efficient adjudication of the claims of the Nationwide Class and Georgia Sub-Class. Plaintiff and the Class members have suffered (and continue to suffer) irreparable harm as a result of Equifax's conduct. The damages suffered by some of the Class members may be relatively small, preventing those Class members from seeking redress on an individual basis for the wrongs alleged herein. Absent a class action, many Class members who suffered damages as a result of the cybersecurity breach of Equifax will not be adequately compensated.

53. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Equifax. Additionally, adjudications with

respect to individual Class members, such as adjudication as to injunctive relief, as a practical matter, would be dispositive of the interests of the other Class members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests.

COUNT ONE

NEGLIGENCE (On behalf of the Nationwide Class)

54. Plaintiff realleges and incorporates all allegations set forth in previous paragraphs as if fully set forth herein.

55. Upon coming into possession of the private, sensitive personal information of Plaintiff's and the Class members, Equifax had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the information from being compromised and/or stolen. Equifax's duty arises from the common law, in part because it was reasonably foreseeable to Equifax that a breach of security was likely to occur under the circumstances and would cause damages to the Nationwide Class as alleged herein.

56. Equifax also had a duty to timely disclose to Plaintiff and Class members that the Equifax Breach had occurred and that the sensitive personal identifying information of the Class members – particularly Social Security numbers, dates of birth, addresses, driver's license numbers, and in some cases sensitive financial information, such as credit card numbers and dispute documents

– had been, or was reasonably believed to be, compromised. Such duty also arises under the common law because it was reasonably foreseeable to Equifax that a breach of security was likely to occur under the circumstances and would cause damages to the Nationwide Class as alleged herein.

57. Equifax, by and through its above negligent acts and/or omissions, further breached its duties to the Class members by failing to timely disclose to Plaintiff and Class members that the Equifax Breach had occurred and that the sensitive personal identifying information of Plaintiff and the Class members had been compromised. Instead, Equifax breached its duty by staying silent about the Equifax Breach for over a month after it was discovered.

58. Equifax also had a duty to put into place internal policies and procedures designed to detect and prevent the unauthorized dissemination of the Plaintiff and Class members' sensitive personal identifying information. Such duty also arises under the common law because it was reasonably foreseeable to Equifax that a breach of security was likely to occur under the circumstances and would cause damages to the Nationwide Class as alleged herein.

59. Equifax, by and through its above negligent acts and/or omissions, unlawfully breach its duties to the Class members by, *inter alia*, failing to exercise reasonable care in protecting and safeguarding the Class members' sensitive personal identifying information within its possession, custody, and control.

60. But for Equifax's negligent and wrongful breach of the duties it owed (and continues to owe) to Plaintiff and the Class members, the cybersecurity breach would not have occurred, and Plaintiff's and the Class members' sensitive personal identifying information would never have been compromised.

61. The Equifax Breach and the above-described substantial injuries suffered by Plaintiff and the Class members as a direct and proximate result of the breach were reasonably foreseeable consequences of Equifax's negligence.

COUNT TWO

NEGLIGENCE PER SE (On behalf of the Nationwide Class)

62. Plaintiff realleges and incorporates all allegations set forth in previous paragraphs as if fully set forth herein.

63. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair...practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect sensitive personal identifying information.

64. In 2007, the FTC published guidelines which establish reasonable data security practices for businesses. The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for

installing vender-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

65. The FTC also has published a document entitled “FTC Facts for Business” which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

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

67. By failing to have reasonable data security measures in place, Equifax engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

68. Equifax’s violation of Section 5 of the FTC Act constitutes negligence *per se*.

69. The Equifax Breach and the above-described substantial injuries suffered by Plaintiff and the Class members as a direct and proximate result of the breach were reasonably foreseeable consequences of Equifax's negligence *per se*.

COUNT THREE

**VIOLATION OF GEORGIA'S DATA BREACH NOTIFICATION
STATUTE, GA. CODE ANN. § 10-1-910, *et seq.*
(On behalf of the Georgia Sub-Class)**

70. Plaintiff realleges and incorporates all allegations set forth in previous paragraphs as if fully set forth herein.

71. Equifax is an "information broker" as defined in Ga. Code Ann. § 10-1-911(3), which "maintains computerized data that includes personal information of individuals." § 10-1-912(a).

72. The sensitive personal identifying information that was comprised by the Equifax Breach, including names, Social Security numbers, birth dates, addresses and driver's license numbers, is "personal information" as defined in Ga. Code Ann. § 10-1-911(6).

73. The Equifax Breach was a "breach of the security of the system" as defined in Ga. Code Ann. § 10-1-911(1).

74. Under Ga. Code Ann. § 10-1-912(a), Equifax was required to "give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state

whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

75. The notice by Equifax “shall be made in the most expedient time possible and without unreasonable delay[.]” § 10-1-912(a)

76. The Equifax Breach impacted more than 10,000 residents of Georgia, and thus, Equifax was further required to “notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis[.]” § 10-1-912(d)

77. According to Equifax, it became aware of the Equifax Breach on July 29, 2017. The Company failed to provide any notice of the Equifax Breach until September 7, 2017.

78. Thus, by failing to disclose the breach in a timely and accurate manner, Equifax violated Ga. Code Ann. § 10-1-912(a) and (d).

79. As a direct and proximate result of Equifax’s violations of Ga. Code Ann. § 10-1-912, Plaintiff and members of the Georgia Sub-Class suffered damages, as described above.

80. Plaintiff and the members of the Georgia Sub-Class seek relief under Ga. Code Ann. § 10-1-912, including, but not limited to, actual damages and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Nationwide Class and Georgia Sub-Class, respectfully requests that the Court certify this action as a class action, with Plaintiff as class representative and the undersigned counsel as class counsel, and enter an order of judgment against Equifax in favor of the Class that, *inter alia*:

- A. awards actual damages to fully compensate the Nationwide Class and Georgia Sub-Class for losses sustained as a direct, proximate, and/or producing cause of Equifax's unlawful conduct;
- B. awards pre-judgment and post-judgment interest at the maximum allowable rates;
- C. awards appropriate injunctive and equitable relief;
- D. awards reasonable attorneys' fees and costs; and
- E. orders any further relief that this Court deems just and proper.

DEMAND FOR JURY TRIAL

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

Dated: October 9th, 2017.

Respectfully submitted,

/s/ Lisa L. Heller

**ROBBINS ROSS ALLOY
BELINFANTE LITTLEFIELD
LLC**

Lisa L. Heller
999 Peachtree Street, N.E. Suite 1120
Atlanta, GA 30309
Tel: (678) 701-9381
Fax: (404) 856-3250

**KESSLER TOPAZ
MELTZER & CHECK LLP**

Naumon A. Amjed
Joshua D'Ancona
Ethan J. Barlieb
Meredith L. Lambert
280 King of Prussia Road
Radnor, PA 19087
Tel: (610) 667-7706
Fax: (610) 667-7056

COOPER & KIRK, PLLC

David H. Thompson
Davis Cooper
1523 New Hampshire Avenue, N.W.
Washington, D.C. 20036
Tel: (202) 220-9600
Fax: (202) 220-9601

Attorneys for Plaintiff Kirby Wilkins

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)

Kirby Wilkins, Individually and On Behalf of
All Others Similarly Situated

DEFENDANT(S)

Equifax, Inc.

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

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT Fulton County, GA
(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)

Naumon A. Amjed - Kessler Topaz Meltzer & Check
280 King of Prussia Road
Radnor, PA 19087 Tel: (610) 667-7706
Local Counsel: Lisa Heller - Robbins Ross, et.al.
1120 Peachtree St., Suite 1120 Atlanta, GA 30309

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION

(PLACE AN "X" IN ONE BOX ONLY)

- 1 U.S. GOVERNMENT PLAINTIFF
- 2 U.S. GOVERNMENT DEFENDANT
- 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- 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 | |
| <input checked="" type="checkbox"/> 1 | <input checked="" type="checkbox"/> 1 | CITIZEN OF THIS STATE | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 | INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE |
| <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | CITIZEN OF ANOTHER STATE | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 | INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE |
| <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | CITIZEN OR SUBJECT OF A FOREIGN COUNTRY | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 | FOREIGN NATION |

IV. ORIGIN (PLACE AN "X" IN ONE BOX ONLY)

- 1 ORIGINAL PROCEEDING
- 2 REMOVED FROM STATE COURT
- 3 REMANDED FROM APPELLATE COURT
- 4 REINSTATED OR REOPENED
- 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District)
- 6 MULTIDISTRICT LITIGATION - TRANSFER
- 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- 8 MULTIDISTRICT LITIGATION - DIRECT FILE

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

This is a class action on behalf of the 143 million individuals whose sensitive personal identifying information was compromised in a cybersecurity breach of Equifax, which was announced September 7, 2017 (the "Equifax Breach"). This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). If a class is certified in this action, the amount in controversy will exceed \$5,000,000.00, exclusive of interest and cost.

(IF COMPLEX, CHECK REASON BELOW)

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

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT \$ _____ APPLYING IFP _____ MAG. JUDGE (IFP) _____
 JUDGE _____ MAG. JUDGE _____ NATURE OF SUIT _____ CAUSE OF ACTION _____
 (Referral)

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

CONTRACT - "0" MONTHS DISCOVERY TRACK

- 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK

- 110 INSURANCE
- 120 MARINE
- 130 MILLER ACT
- 140 NEGOTIABLE INSTRUMENT
- 151 MEDICARE ACT
- 160 STOCKHOLDERS' SUITS
- 190 OTHER CONTRACT
- 195 CONTRACT PRODUCT LIABILITY
- 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- 210 LAND CONDEMNATION
- 220 FORECLOSURE
- 230 RENT LEASE & EJECTMENT
- 240 TORTS TO LAND
- 245 TORT PRODUCT LIABILITY
- 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK

- 310 AIRPLANE
- 315 AIRPLANE PRODUCT LIABILITY
- 320 ASSAULT, LIBEL & SLANDER
- 330 FEDERAL EMPLOYERS' LIABILITY
- 340 MARINE
- 345 MARINE PRODUCT LIABILITY
- 350 MOTOR VEHICLE
- 355 MOTOR VEHICLE PRODUCT LIABILITY
- 360 OTHER PERSONAL INJURY
- 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- 365 PERSONAL INJURY - PRODUCT LIABILITY
- 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- 370 OTHER FRAUD
- 371 TRUTH IN LENDING
- 380 OTHER PERSONAL PROPERTY DAMAGE
- 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK

- 422 APPEAL 28 USC 158
- 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK

- 440 OTHER CIVIL RIGHTS
- 441 VOTING
- 442 EMPLOYMENT
- 443 HOUSING/ ACCOMMODATIONS
- 445 AMERICANS with DISABILITIES - Employment
- 446 AMERICANS with DISABILITIES - Other
- 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK

- 462 NATURALIZATION APPLICATION
- 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK

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

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK

- 550 CIVIL RIGHTS - Filed by Counsel
- 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK

- 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK

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

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK

- 820 COPYRIGHTS
- 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK

- 830 PATENT
- 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDA) - a/k/a Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK

- 861 HIA (1395f)
- 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 ANITRUST
- 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 DEMANDS _____

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

VIII. RELATED/REFILED CASE(S) IF ANY

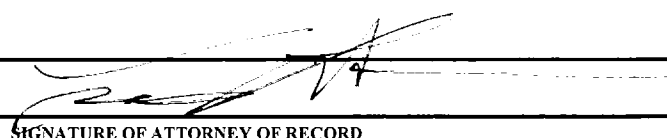
JUDGE Duffy and Totenberg DOCKET NO. 1:17cv3433/1:17cv3448

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)):

Randolph Jefferson Cary II; William R. Porter; Robin D. Porter, individually, and on behalf of all others similarly situated v. Equifax Inc. Nida Samson, et. al. v. Equifax

- 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.



10/9/17

SIGNATURE OF ATTORNEY OF RECORD

DATE