

\$5,000,000, exclusive of interest and costs, and members of the Class are citizens of states different from the Defendant.

5. This Court has personal jurisdiction over Defendant because it regularly conducts business within the State of Alabama in the form of providing ride-sharing services.

6. Venue is proper in this District pursuant to 28 USC §1391(b)(1) because Defendant resides in said district, and under 28 USC § 1391(b)(2) because a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL BACKGROUND

7. Plaintiff brings this class action against the Defendant for its failure to secure and safeguard her personal identifying information (“Private Information”), and that of the some 57 million similarly-situated people who either drove for Defendant or used its services as riders, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their Private Information had been stolen and precisely what types of information was stolen.

8. Defendant develops, markets, and operates a mobile-app-based transportation network called Uber. The Uber app allows riders to submit a trip request by smartphone, which is routed to Defendant's drivers.

9. Defendant's business depends on drivers, who must provide their Private Information, including extremely sensitive Private Information such as their Social Security Numbers, to Defendants in order to work as drivers and earn a livelihood.

10. Riders must also provide Private Information in order to use Uber's services, including financial information that is required to pay for rides through Defendant's app.

A. Defendant Failed to Notify Class Members About a Massive Data Breach in 2016, Instead Paying Hackers to Cover It Up.

11. On November 21, 2017, news reports were published that made public, for the first time, that Defendant suffered a massive data breach in October 2016, in which Private Information of some 57 million of Defendant's riders and drivers was accessed by hackers (the “2016 Data Breach”). *See, e.g.,* <https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data>.

12. Defendant learned about the 2016 Data Breach by November 2016, but purposely chose not to notify those whose Private Information was compromised at that time.

13. Instead of notifying the victims of the 2016 Data Breach about it, Defendant paid hackers who perpetrated it \$100,000 in an effort to cover up the 2016 Data Breach. *Id.*

14. Defendant thus conspired with the hackers who perpetrated the 2016 Data Breach to keep its victims – Defendant's drivers and riders – ignorant about it.

15. According to the news reports, the 2016 Data Breach occurred when two hackers “accessed a private GitHub coding site used by Uber software engineers and then used login credentials they obtained there to access data stored on the Amazon Web Services account that handled computing tasks for the company. From there, the hackers discovered an archive of rider and driver information. Later, they emailed Uber asking for money, according to the company.” *Id.*

16. “Compromised data from the October 2016 attack included names, email addresses and phone numbers of 50 million Uber riders around the world, the company told Bloomberg on Tuesday. The Private Information of about 7 million drivers was accessed as well, including some 600,000 U.S. driver's license numbers. No Social Security numbers, credit card information, trip location details or other data were taken, Uber said.” *Id.*

17. According to news reports, Defendant's board of directors commissioned an investigation into the activities of its security team in or around October 2017, which team was led by Defendant's Chief Security Officer, Joe Sullivan. This project, conducted by an outside law firm, discovered the 2016 Data Breach and the failure to disclose it. *Id.*

18. In response to this discovery, Cara Khosrowshahi, who has been Defendant's CEO since August 2017, asked for the resignation of Mr. Sullivan and fired Craig Clark, a senior lawyer who reported to Mr. Sullivan. *Id.*

19. As these news reports surfaced, Defendant published several statements concerning the 2016 Data Breach on its own website, confirming much of what was published in news reports.

20. According to one of Defendant's statements concerning the 2016 Data Breach: “Driver information included the names, email addresses and mobile phone numbers related to accounts globally. In addition, the driver's license numbers of around 600,000 drivers in the United States were downloaded. <<https://help.uber.com/h/04d4d787-ca99-40a3-ab27-9af42d196575>>.”

21. Defendant has yet to provide any direct notification to victims of the 2016 Data Breach that their Private Information was compromised.

B. Defendant Also Failed to Notify Class Members about a 2014 Data Breach that Preceded, and Was Similar in Many Ways to, the 2016 Data Breach.

22. At the time Defendant discovered the 2016 Data Breach and made the illegal and reprehensible decision not to disclose it, Defendant had recently settled a lawsuit with the New York Attorney General over a very similar data breach that occurred in 2014 (the “2014 Data Breach”), and

was in the process of negotiating with the Federal Trade Commission over its handling of consumer data.

23. In the 2014 Data Breach, much like the 2016 Data Breach, one or more hackers utilized credentials that defendant made available one or more GitHub web-pages (and/or via the GitHub app, which is an app designed for sharing code among app developers). *See*, e.g., <https://www.theregister.co.uk/2015/02/28/uber_subpoenas_github_for_hacker_details>.

24. Defendant did not disclose the 2014 Data Breach until February 27, 2015, when it disseminated a Press Release stating, *inter alia*, “In late 2014, we identified a one-time access of an Uber database by an unauthorized third party....” (the “2015 Press Release”).

25. Defendant admitted in its 2015 Press Release that it knew of the 2014 Data Breach at least as early as September 17, 2014 – over five months before Defendant issued the 2015 Press Release or made any effort whatsoever to notify those affected that their Private Information had been disclosed in the Data Breach. *Id.*

26. Defendant's 2015 Press Release further stated that “unauthorized access to an Uber database by a third party . . . occurred on May 13, 2014,” and that “the unauthorized access impacted approximately 50,000 drivers across multiple states.” *Id.*

27. Defendant's initial representations about the 2014 Breach indicated, much as its current representations concerning the 2016 Data Breach indicate, that only drivers' license numbers and names were disclosed in the 2014 Data Breach. However, this turned out not to be true.

28. In or around August 2016 – approximately two years after the 2014 Data Breach, and shortly before Defendant's discovery of the 2016 Data Breach – Defendant issued more notifications to the victims of the 2014 Data Breach informing them that, contrary to its earlier representations and notices, additional Private Information was disclosed in the 2014 Data Breach (the “Second 2014 Breach Notification”).

29. In its Second 2014 Breach Notifications Defendant revealed that, contrary to its initial representations concerning the scope of the 2014 Data Breach, additional Private Information was disclosed in the 2014 Data Breach, including banking information and Social Security Numbers, in addition to driver's license numbers and names.

C. Plaintiff Was Injured by the 2016 Data Breach

30. Defendant has repeatedly disregarded Plaintiff's and Class Members' rights by intentionally, willfully, and recklessly failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the 2016 Data Breach

from ever happening, despite its experience with the 2014 Data Breach (which both occurred because Defendant made credentials available through GitHub websites), and failing to disclose to those affected the facts that it did not have adequate computer systems and security practices in place, or that the Data Breach had occurred in a timely manner. On information and belief, Plaintiff's and Class Members' Private Information and the password allowing access to that Private Information were improperly handled and stored, were unencrypted, and were not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiff's and Class Members' Private Information was compromised and stolen.

31. Disclosure of the types of Private Information that Defendant admits were compromised in the 2016 Data Breach presents a danger to victims of the breach. Information such as data breach victims' names, birth dates, email addresses, and other identifying information alone creates a material risk of identity theft. Identity thieves can use such Private Information to locate additional Private Information, such as financial information and Social Security Numbers, and use the combined information to perpetrate fraud such as, for instance, opening new financial accounts in victims' names, or filing false tax returns in victims' names and collecting the tax refunds.

32. However, given the facts surrounding the 2014 and 2016 Data Breaches, Defendant's current representations concerning the scope of the 2016 Data Breach cannot be accepted as true. Defendant possesses a wide variety of Private Information concerning Class Members, and repeatedly has failed to protect that Private Information. Based on the facts alleged above, Plaintiff assumes that all the Private Information that Defendant has about them has been handled incompetently and improperly, and Plaintiff must assume that all of the Private Information in Defendant's possession has been obtained by hackers who either will misuse that Private Information themselves or sell it to others to who will do so, if this has not already occurred. There is no expiration on how long victims' Private Information can stay in the hands of identity thieves before it is misused.

33. Plaintiff and other Class Members suffered injuries including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, invasion of their privacy, and loss of value of their Private Information.

34. It is well known and the subject of many media reports that Private Information like that taken in the Data Breach at issue is highly coveted and a frequent target of hackers.

35. Legitimate organizations and the criminal underground alike recognize the value in such Private Information. Otherwise, they wouldn't pay for it or aggressively seek it.

36. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." Verizon 2014 PCI Compliance Report, available at

<http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.p 21 df>
(hereafter "2014 Verizon Report").

37. The ramifications of Defendant's failure to keep Class Members' data secure are severe.

38. There is a strong likelihood that Class Members will become victims of identity fraud in the future given the breadth of their Private Information that is now available to ID thieves and other criminals on the dark web. For instance, According to a Javelin Strategy and Research Study, 16% of all Americans have been victims of identity theft as of 2016. <<https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new>> .

39. As the FTC recognizes, once identity thieves have Private Information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."

40. Identity thieves can use Private Information such as that of Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

41. In addition, identity thieves may get medical services using consumers' compromised Private Information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

42. Plaintiff and other Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges that may be incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

43. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and other Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. theft of their Private Information;
- b. damage to Plaintiff's and Class Members' credit reports and/or scores;
- c. the untimely and inadequate notification of the Data Breach;
- d. loss of privacy;

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

CLASS ACTION ALLEGATIONS

44. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of herself and the following proposed classes:

National Class: All persons residing in the United States whose Private Information was disclosed in the data breach in 2016.

Alabama Consumer Subclass: All members of the Nationwide Consumer Class who are residents of Alabama who purchased Uber services in Alabama.

45. Excluded from the Class are Defendant, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

46. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiff at this time, based on Defendant's statements Private Information pertaining to approximate 57 million riders and drivers, globally, was disclosed in the Data Breach.

47. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant has an express or implied contractual obligation to use reasonable security measures;
- b. Whether Defendant complied with any express or implied contractual obligation to use reasonable security measures; ;
- c. Whether Defendant violated the Deceptive Trade Practices Act, Ala. Code (1975) § 8-19-1 *et seq.*
- d. What security procedures and data-breach notification procedure should Defendant be required to implement as part of any injunctive relief ordered by the Court;
- e. The nature of the relief, including equitable relief, to which Plaintiff and the Class members are entitled.

48. Ascertainability. All members of the purposed Class are readily ascertainable. Defendant

has access to addresses and other contact information for all, or substantially all, members of the Class, which can be used for providing notice to many Class Members.

49. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other class member, was misused and/or disclosed by Defendant.

50. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

51. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted 18 claims. There will be no difficulty in the management of this action as a class action.

52. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

53. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and 24 (b)(2), because Defendant has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I

Negligence

On Behalf of the National Class and Each Subclass

54. Plaintiff realleges and incorporates the preceding factual allegations as if fully set forth herein.

55. Defendant actively solicited Plaintiff and the other Class Members to use their Private Information in transactions with Uber.

56. When Plaintiff and the other Class Members gave their Private Information to Defendant to facilitate and close transactions, they did so with the mutual understanding that Defendant had reasonable security measures in place and would take reasonable steps to protect and safeguard the Private Information of Plaintiff and the other Class Members.

57. Plaintiff and the other Class Members also gave their Private Information to Defendant on the premise that Defendant was in a superior position to protect against the harms attendant to unauthorized access, theft and misuse of that information.

58. Upon accepting Plaintiff's and Class Members' Private Information in their respective point-of-sale systems, Uber undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties, and to utilize commercially reasonable methods to do so.

59. This duty included, among other things, designing, maintaining, and testing Uber's security systems to ensure that Plaintiff's and the Class Members' Private Information was adequately secured and protected.

60. Uber further had a duty to implement processes that would detect a breach of its security system in a timely manner.

61. Uber had a duty to timely disclose to Plaintiff and Class Members that their Private Information had been or was reasonably believed to have been compromised. Timely disclosure was appropriate so that, among other things, Plaintiff and Class Members could take appropriate measures to avoid use of bank funds, and monitor their account information and credit reports for fraudulent activity.

62. Uber breached its duty to discover and to notify Plaintiff and Class Members of the unauthorized access by failing to discover the security breach within reasonable time and by failing to notify Plaintiff and Class Members of the breach until November of 2017.

63. Uber also breached its duty to Plaintiff and Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its negligent practices, Uber failed to provide adequate supervision and oversight of the Private Information with which it is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiff's and Class Members' Private Information, misuse the Private Information, and intentionally disclose it to others without consent.

64. Through Uber's acts and omissions described in this Complaint, including Uber's failure to provide adequate security and its failure to protect Plaintiff's and Class Members' Private Information from being foreseeably captured, accessed, disseminated, stolen, and misused, Uber unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' Private Information during time it was within Uber's control.

65. Further, through its failure to timely discover and provide clear notification of the data breach to consumers and driver, Uber prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their Private Information.

66. Upon information and belief, Uber improperly and inadequately safeguarded the Personal Information of Plaintiff and Class Members in deviation from standard industry rules, regulations, and practices at the time of the data breach.

67. Uber's failure to take proper security measures to protect Plaintiff's and Class Members' sensitive Private Information as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' Private Information.

68. Uber's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information; failing to conduct adequate regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class Members' Private Information.

69. Neither Plaintiff nor the other Class Members contributed to the data breach and subsequent misuse of their Private Information as described in this Complaint. As a direct and proximate result of Uber's negligence, Plaintiff and Class Members sustained actual losses and damages as described in detail above.

COUNT II
BREACH OF IMPLIED CONTRACT
On Behalf of Nationwide Class and Each Subclass

70. Plaintiff realleges and incorporates the preceding factual allegations as if fully set forth herein.

71. Uber's system solicited and invited Plaintiff and the members of the Class to book rides, and for drivers to drive customers.

72. Plaintiff and Class Members accepted Uber's offers and booked rides through Uber.

73. When Plaintiff and Class Members booked rides through Uber, they provided their Private Information. In so doing, Plaintiff and Class Members entered into implied contracts with Uber to which Uber agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised.

74. Each booking made with Uber's system by Plaintiff and Class Members was made pursuant to the mutually agreed-upon implied contract with Uber and the drivers using their system under which Uber agreed to safeguard and protect Plaintiff's and Class Members' Private Information and to timely and accurately notify them if such information was compromised or stolen.

75. Plaintiff and Class Members would not have provided and entrusted their Private

Information to Uber in the absence of the implied contract between them and Uber.

76. Plaintiff and Class Members fully performed their obligations under the implied contracts with Uber.

77. Uber breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the Private Information of Plaintiff and Class Members and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the data breach.

78. As a direct and proximate result of Uber's breaches of the implied contracts between Uber and Plaintiff and Class Members, Plaintiff and Members sustained actual losses and damages as described in detail above.

**COUNT III
UNJUST ENRICHMENT
On Behalf of Nationwide Class and Each Subclass**

79. Plaintiff realleges and incorporates the preceding factual allegations as if fully set forth herein.

80. Uber has received and retained a benefit from Plaintiff and the Class Members and inequity has resulted.

81. Uber has benefited from providing a service without paying for adequate security and Plaintiff and Class Members have overpaid for a service that is not in fact secure.

82. Thus, Class Members conferred a benefit on Uber by paying full price for a service that had already been exposed by criminals.

83. It is inequitable for Uber to retain these benefits.

84. Plaintiff were not aware of the true facts about the data breach until over a year later, and did not benefit from Uber's conduct.

85. Uber knowingly accepted the benefits of its unjust conduct.

86. As a result of Uber's conduct, the amount of its unjust enrichment should be disgorged, in an amount according to proof .

COUNT IV
VIOLATION OF ALABAMA DECEPTIVE TRADE PRACTICES ACT,
Ala. Code § 8-19-1, On Behalf of Alabama Subclass

87. Plaintiff realleges and incorporates the preceding factual allegations as if fully set forth herein.

88. The Alabama Deceptive Trade Practices Act, Alabama Code § 8-19-1 *et seq.* (the “Alabama Deceptive Trade Practices Act” or “ADTPA”) and specifically subsection 8-19-5(27), prohibits any “unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.” Uber engaged in conduct that violated this subsection of the statute.

89. Uber committed an unlawful business act or practice in violation of the ADTPA when it failed to disclose to Plaintiff and member of the Alabama subclass that their Private Information was in the hands of criminals.

90. Uber committed unfair and fraudulent business acts and practices in violation of the ADTPA when it affirmatively misrepresented, actively concealed, and/or failed to disclose the truth of the data breach detailed herein.

91. Uber committed unfair and fraudulent business acts and practices in violation of the ADTPA when it failed to secure customer data and instead paid and failed to disclose the payment of a \$100,000 ransom to criminals who stole customer and driver Private Information.

92. Uber disseminated unfair, deceptive, untrue and/or misleading statements regarding the security of Uber.

93. In addition, Uber engaged in unlawful acts and practices with respect to its services by failing to discover and then disclose the data breach to Plaintiff and Class Members in a timely and accurate manner, contrary to the duties imposed by the ADTPA.

94. Uber knew or should have known that its system had been breached and data security practices were inadequate to safeguard Class Members’ Private Information and that the risk of a data breach or theft was highly likely. Uber’s actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Class Members.

95. Uber’s unfair or deceptive acts or practices occurred repeatedly in the course of Uber’s trade or business in Alabama, and were capable of deceiving a substantial portion of the purchasing public nationwide.

96. As a direct and proximate result of Uber’s unfair and deceptive practices, Plaintiff and Class Members have suffered and will continue to suffer actual damages.

98. As a result of its unfair and deceptive conduct, Uber has been unjustly enriched and should be required to make restitution to Plaintiff and Class Members pursuant to the ADTPA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Nationwide Class and the Alabama Subclass proposed in this Complaint, respectfully request that this Honorable Court enter judgment in their favor and against Uber as follows:


- a. For an Order certifying the Classes, as defined herein, and appointing Plaintiff and her Counsel to represent the Nationwide Class and/or the Alabama Subclass;
- b. For equitable relief enjoining Uber from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' personal information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class members;
- c. For equitable relief compelling Uber to use appropriate cyber security methods and policies with respect to its data collection, storage and protection and to disclose with specificity to Class members the type of personal information compromised;
- d. For an award of compensatory and punitive damages, as allowed by law in an amount to be determined;
- e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;
- f. For prejudgment interest on all amounts awarded; and
- g. Such other, further, and different relief as this Honorable Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand trial by struck jury.

Respectfully submitted this 19 day of January, 2018.

OF COUNSEL FOR PLAINTIFFS:

/LRS/  _____ Leon R. Storie

Leon R. Storie, Esq. ASB-4172-E37L
Leon Storie, Attorney at Law 2821 7th Street
Tuscaloosa, Alabama 35401 Telephone 205-737-0318 Fax 205-210-4651
email: leon@leonstorie.com

Gregory Law Firm, P.C.
2700 Corporate Drive
Suite 200
Birmingham, Alabama 35242 Telephone 205-799-0380
email: steve@gregorylawfirm.us
ASB-0737-R73S

DEFENDANT TO BE SERVED VIA PROCESS SERVER:

UBER TECHNOLOGIES, INC.
800 Market Street, 7th Floor,
San Francisco, CA 94012.

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Claims Uber Attempted to Cover Up 2016 Data Breach](#)
