

EXHIBIT B



**Service of Process
Transmittal**

11/30/2017
CT Log Number 532389074

TO: Max Watkins
UBER TECHNOLOGIES, INC.
1455 Market St Fl 4
San Francisco, CA 94103-1355

RE: Process Served in California

FOR: UBER TECHNOLOGIES, INC. (Domestic State: DE)

ENCLOSED ARE COPIES OF LEGAL PROCESS RECEIVED BY THE STATUTORY AGENT OF THE ABOVE COMPANY AS FOLLOWS:

TITLE OF ACTION: Karl J. Nicolai, etc., Pltf. vs. UBER TECHNOLOGIES, INC., et al., Dfts.

DOCUMENT(S) SERVED: Letter, Cover Sheet, Summons, Complaint, Exhibit(s)

COURT/AGENCY: Richland County - Court of Common Pleas, SC
Case # 2017CP4007129

NATURE OF ACTION: NEGLIGENCE, GROSS NEGLIGENCE, RECKLESSNESS, NEGLIGENT HIRING, NEGLIGENT TRAINING AND NEGLIGENT SUPERVISION

ON WHOM PROCESS WAS SERVED: C T Corporation System, Los Angeles, CA

DATE AND HOUR OF SERVICE: By Certified Mail on 11/30/2017 postmarked: "Not Post Marked"

JURISDICTION SERVED : California

APPEARANCE OR ANSWER DUE: Within 30 days after service, exclusive of the day of service

ATTORNEY(S) / SENDER(S): David Proffitt
PROFFITT & Cox, LLP
140 Wildewood Park Drive, Suite A
Columbia, SC 29223
803-834-7097

ACTION ITEMS: CT has retained the current log, Retain Date: 12/01/2017, Expected Purge Date: 12/06/2017

Image SOP

Email Notification, Max Watkins mwatkins@uber.com

Email Notification, Dylan Tonti tonti@uber.com

Email Notification, Allison Garrett agarrett@uber.com

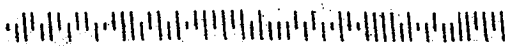
Email Notification, Rose Barajas rbarajas@uber.com

SIGNED: C T Corporation System

ADDRESS: 818 West Seventh Street
Los Angeles, CA 90017

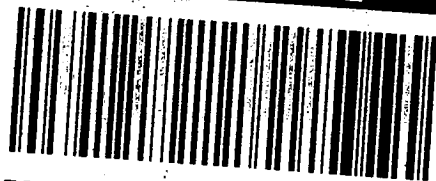
TELEPHONE: 213-337-4615

Information displayed on this transmittal is for CT Corporation's record keeping purposes only and is provided to the recipient for quick reference. This information does not constitute a legal opinion as to the nature of action, the amount of damages, the answer date, or any information contained in the documents themselves. Recipient is responsible for interpreting said documents and for taking appropriate action. Signatures on certified mail receipts confirm receipt of package only, not contents.



PROFFITT & COX, LLP
Attorneys at Law
Wildewood Business Center
140 Wildewood Park Dr. Suite A
Columbia, South Carolina 29223

PLACE STICKER AT TOP OF ENVELOPE TO THE RIGHT
OF THE RETURN ADDRESS. FOLD AT DOTTED LINE
CERTIFIED MAIL



7015 3010 0001 4031 0860

Uber Technologies, Inc.
c/o CT Corporation System, Its Registered Agent
818 West Seventh St., Suite 930
Los Angeles, CA 90017

PROFFITT & COX

Attorneys at Law

PROFFITT & COX, LLP
140 WILDEWOOD PARK DRIVE, SUITE A
COLUMBIA, SC 29223-4311
TELEPHONE (803) 834-7097
FACSIMILE (888) 711-1057
WWW.PROFFITTCOX.COM

DAVID PROFFITT
dproffitt@proffittcox.com

BY CERTIFIED U.S. MAIL / RETURN RECEIPT REQUESTED

November 27, 2017

Uber Technologies, Inc.
c/o CT Corporation System, Its Registered Agent
818 West Seventh St., Suite 930
Los Angeles, CA 90017

Uber Technologies, Inc.
c/o The Corporation Trust Company, Its Registered Agent
Corporation Trust Center
1209 Orange St.
Wilmington, DE 19801

Rasier, LLC
c/o CT Corporation System, Its Registered Agent
2 Office Park Court, Suite 103
Columbia, SC 29223

RE: Karl J. Nicolai v. Uber Technologies, Inc., Rasier, LLC, and John Does 1 through 10
C.A. No. 2017-CP-40-07129
PC File No. 1562.00

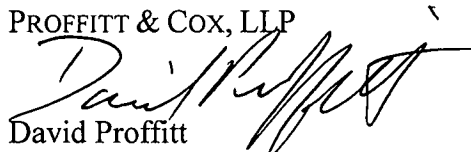
Dear Registered Agent:

Please find enclosed for service on you, as registered agent for the above-named Defendants, a Summons and Class Action Complaint filed November 22, 2017, in Richland County Court of Common Pleas in South Carolina.

With kindest personal regards, I remain

Sincerely yours,

PROFFITT & COX, LLP


David Proffitt

RDP/nif
Enclosures

STATE OF SOUTH CAROLINA)
COUNTY OF RICHLAND)

IN THE COURT OF COMMON PLEAS

Karl J. Nicolai, individually and on behalf of all others
similarly situated,)

CIVIL ACTION COVERSHEET

Plaintiff(s))

vs.)

Uber Technologies, Inc. and Raiser, LLC, and John
Does 1 through 10,)

Defendant(s))

2017-CP-400-7129

Submitted By: R. David Proffitt
Address: PROFFITT & COX, LLP
140 Wildewood Park Dr. Suite A
Columbia, South Carolina 29223

SC Bar #: 11193
Telephone #: 803-834-7097
Fax #: 888-711-1057
Other:
E-mail: dproffitt@proffittcox.com

NOTE: The coversheet and information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is required for the use of the Clerk of Court for the purpose of docketing. It must be filled out completely, signed, and dated. A copy of this coversheet must be served on the defendant(s) along with the Summons and Complaint.

DOCKETING INFORMATION (Check all that apply)

*If Action is Judgment/Settlement do not complete

- JURY TRIAL demanded in complaint.
NON-JURY TRIAL demanded in complaint.
This case is subject to ARBITRATION pursuant to the Court Annexed Alternative Dispute Resolution Rules.
This case is subject to MEDIATION pursuant to the Court Annexed Alternative Dispute Resolution Rules.
This case is exempt from ADR. (Proof of ADR/Exemption Attached)

NATURE OF ACTION (Check One Box Below)

- Contracts: Constructions (100), Debt Collection (110), General (130), Breach of Contract (140), Fraud/Bad Faith (150), Failure to Deliver/Warranty (160), Employment Discrim (170), Employment (180), Other (199)
Torts - Professional Malpractice: Dental Malpractice (200), Legal Malpractice (210), Medical Malpractice (220), Previous Notice of Intent Case # 20-NI-, Notice/ File Med Mal (230), Other (299)
Torts - Personal Injury: Conversion (310), Motor Vehicle Accident (320), Premises Liability (330), Products Liability (340), Personal Injury (350), Wrongful Death (360), Assault/Battery (370), Slander/Label (380), Other (399)
Real Property: Claim & Delivery (400), Condemnation (410), Foreclosure (420), Mechanic's Lien (430), Partition (440), Possession (450), Building Code Violation (460), Other (499)
Inmate Petitions: PCR (500), Mandamus (520), Habeas Corpus (530), Other (599)
Administrative Law/Relief: Reinstate Drv. License (800), Judicial Review (810), Relief (820), Permanent Injunction (830), Forfeiture-Petition (840), Forfeiture-Consent Order (850), Other (899)
Judgments/Settlements: Death Settlement (700), Foreign Judgment (710), Magistrate's Judgment (720), Minor Settlement (730), Transcript Judgment (740), Lis Pendens (750), Transfer of Structured Settlement Payment Rights Application (760), Confession of Judgment (770), Petition for Workers Compensation Settlement Approval (780), Other (799)
Appeals: Arbitration (900), Magistrate-Civil (910), Magistrate-Criminal (920), Municipal (930), Probate Court (940), SCDOT (950), Worker's Comp (960), Zoning Board (970), Public Service Comm. (990), Employment Security Comm (991), Other (999)
Special/Complex /Other: Environmental (600), Automobile Arb. (610), Medical (620), Other (699), Sexual Predator (510), Permanent Restraining Order (680), Pharmaceuticals (630), Unfair Trade Practices (640), Out-of State Depositions (650), Motion to Quash Subpoena in an Out-of-County Action (660), Pre-Suit Discovery (670)

2017 NOV 22 2 03 PM
RICHLAND COUNTY
FILED

Submitting Party Signature:

David Proffitt

Date: 11/22/2017

Note: Frivolous civil proceedings may be subject to sanctions pursuant to SCRCP, Rule 11, and the South Carolina Frivolous Civil Proceedings Sanctions Act, S.C. Code Ann. §15-36-10 et. seq.

Effective January 1, 2016, Alternative Dispute Resolution (ADR) is mandatory in all counties, pursuant to Supreme Court Order dated November 12, 2015.

SUPREME COURT RULES REQUIRE THE SUBMISSION OF ALL CIVIL CASES TO AN ALTERNATIVE DISPUTE RESOLUTION PROCESS, UNLESS OTHERWISE EXEMPT.

Pursuant to the ADR Rules, you are required to take the following action(s):

1. The parties shall select a neutral and file a "Proof of ADR" form on or by the 210th day of the filing of this action. If the parties have not selected a neutral within 210 days, the Clerk of Court shall then appoint a primary and secondary mediator from the current roster on a rotating basis from among those mediators agreeing to accept cases in the county in which the action has been filed.
2. The initial ADR conference must be held within 300 days after the filing of the action.
3. Pre-suit medical malpractice mediations required by S.C. Code §15-79-125 shall be held not later than 120 days after all defendants are served with the "Notice of Intent to File Suit" or as the court directs.
4. Cases are exempt from ADR only upon the following grounds:
 - a. Special proceeding, or actions seeking extraordinary relief such as mandamus, habeas corpus, or prohibition;
 - b. Requests for temporary relief;
 - c. Appeals
 - d. Post Conviction relief matters;
 - e. Contempt of Court proceedings;
 - f. Forfeiture proceedings brought by governmental entities;
 - g. Mortgage foreclosures; and
 - h. Cases that have been previously subjected to an ADR conference, unless otherwise required by Rule 3 or by statute.
5. In cases not subject to ADR, the Chief Judge for Administrative Purposes, upon the motion of the court or of any party, may order a case to mediation.
6. Motion of a party to be exempt from payment of neutral fees due to indigency should be filed with the Court within ten (10) days after the ADR conference has been concluded.

Please Note: You must comply with the Supreme Court Rules regarding ADR. Failure to do so may affect your case or may result in sanctions.

STATE OF SOUTH CAROLINA
COUNTY OF RICHLAND

IN THE COURT OF COMMON PLEAS
C.A. No. _____

Karl J. Nicolai, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

Uber Technologies, Inc. and Rasier, LLC,
and John Does 1 through 10,

Defendants.

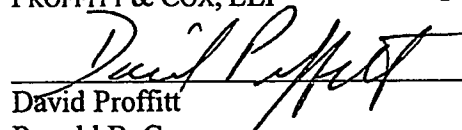
RICHLAND COUNTY
FILED
2017 NOV 22 PM 4:39
JEANNETTE W. MORRIS
C.C.P. 2.65.

SUMMONS

TO: UBER TECHNOLOGIES, INC. AND RASIER, LLC

YOU ARE HEREBY SUMMONED and required to answer the Complaint herein, a copy of which is herewith served upon you, and to serve a copy of your Answer to said Complaint upon the subscriber at his office at 140 Wildewood Park Drive, Suite A, Columbia, South Carolina, 29223 within thirty (30) days after the service hereof, exclusive of the day of such service, and if you fail to answer the Complaint within the time aforesaid, judgment by default will be rendered against you for the relief demanded in the Complaint.

PROFFITT & COX, LLP


David Proffitt

Ronald B. Cox
140 Wildewood Park Drive, Suite A
Columbia, S.C. 29223-6518
Telephone: (803) 834-7097
Fax: (888) 711-1057
Email: dproffitt@proffittcox.com
Email: rcox@proffittcox.com

Attorneys for Plaintiffs

November 22, 2017

STATE OF SOUTH CAROLINA

IN THE COURT OF COMMON PLEAS

COUNTY OF RICHLAND

C.A. No. _____

Karl J. Nicolai, individually and on behalf of
all others similarly situated,

Plaintiff,

v.

Uber Technologies, Inc. and Rasier, LLC,
and John Does 1 through 10,

Defendants.

RICHLAND COUNTY
FILED
2017 NOV 22 PM 4:39
JEANETTE W. JOHNSON
Clerk of Court

CLASS ACTION COMPLAINT
(JURY TRIAL DEMANDED)

Plaintiff, by and through his undersigned counsel, complaining of the Defendants, states the following allegations. Plaintiff's allegations and claims are made individually and on behalf of all others similarly situated.

PARTIES AND JURISDICTION

1. Plaintiff Karl J. Nicolai is a resident of Richland County, South Carolina, and has worked as a driver for Defendants and also has used Defendants' services as a user and passenger in South Carolina.

2. On information and belief, Defendant Uber Technologies, Inc., is a corporation headquartered in San Francisco, California, and incorporated or organized under the laws of the state of Delaware.

3. On information and belief, Defendant Rasier, LLC, is a limited liability company headquartered in San Francisco, California, and incorporated or organized under the laws of the state of Delaware (hereinafter, collectively, “Defendants” or “Uber”).

4. On information and belief, John Does 1 through 10 are persons or entities, presently unknown to Plaintiff, who may be involved and liable for the wrongful actions and omissions as described herein.

5. This Court, as a court of general jurisdiction in South Carolina, has subject matter jurisdiction over this lawsuit and personal jurisdiction over the parties.

6. Venue is proper in this Court. Defendants do business in Richland County and throughout the state of South Carolina. Defendants and their employees and agents conduct substantial business in Richland County. Defendants transact business, committed a negligent or wrongful act in, maintain agents or representatives in, or are found in Richland County.

FACTUAL ALLEGATIONS

7. Defendants are privately held entities which provides computer and mobile phone applications which allow a user to identify and communicate with a driver with a vehicle to transport the user from one destination to another.

8. On information and belief, persons who wish to work as a driver for Defendants using their own vehicle must undergo a background check and screening process and must provide, among other things, their name, address, email address, telephone number, driver’s license, Social Security number, financial account information, vehicle registration, proof of insurance, proof of vehicle inspection and must have a vehicle meeting specified requirements.

9. On information and belief, persons who wish to use Defendants' services as a passenger must provide personal, private information to Defendants, including, among other things, their name, address, email address and financial account information.

10. On information and belief, the data held by Defendants includes information containing the personal, private information of Plaintiff and millions of other Uber drivers and users. The data includes such items as names, addresses, email addresses, telephone numbers, account passwords, security questions, Social Security numbers, driver's license numbers, birth dates, financial account information, vehicle registration and insurance information and other private, personal information.

11. On information and belief, Defendants' drivers throughout South Carolina use Defendants' computer and mobile phone applications to identify and communicate with persons requesting a ride. The on-demand system enables users to hail a car service using Defendants' applications, and which enables the drivers to fulfill such requests for transportation services.

12. At all relevant times, Defendants and their employees and agents distributed, implemented, warranted, permitted, license or otherwise caused their applications and services to be used by drivers and users throughout South Carolina.

13. On information and belief, there were more than 327,000 Uber drivers in the United States as of 2015, including Plaintiff and a large and substantial number of drivers throughout South Carolina.

14. On information and belief, Uber users throughout South Carolina use Uber's computer and mobile phone applications to identify and communicate with Uber drivers.

15. On information and belief, there were nearly 16 million monthly active users of Uber's services in the United States as of 2016, including Plaintiff and a large and substantial number of users throughout South Carolina.

16. On or about November 21, 2017, Dara Khosrowshahi, chief executive officer of Uber Technologies, for the first time publicly revealed in a statement posted on Uber's website that "in late 2016 we became aware that two individuals outside the company had inappropriately accessed user data stored on a third-party cloud-based service that we use."

17. Khosrowshahi stated that "individuals were able to download files containing a significant amount of other information, including: The names and driver's license numbers of around 600,000 drivers in the United States. . . . [and] [s]ome personal information of 57 million Uber users around the world, including the drivers described above. This information included names, email addresses and mobile phone numbers. . . ." (Statement of Khosrowshahi attached as EXHIBIT A.)

18. On information and belief, Travis Kalanick, Defendants' co-founder and former chief executive, became aware of the breach a month after it occurred. Instead of reporting the attack to regulators and victims last year, Defendants paid hackers \$100,000 to delete the data and keep the security breach under wraps.

19. On information and belief, the security breach resulted in the theft of personal identifying information held by Defendants about their drivers and users in South Carolina.

20. On information and belief, Defendants asserted and admitted that they never notified any Uber driver or user about the security breach until November 21, 2017, even though it occurred about one year ago. Khosrowshahi stated, "You may be asking why we are just talking about this now, a year later. I had the same question, so I immediately asked for a thorough

investigation of what happened and how we handled it.” (Statement of Khosrowshahi attached as EXHIBIT A.)

21. On information and belief, Defendants did not properly and timely notify Plaintiff or any of their drivers and users in South Carolina about the security breach which it admits occurred about a year ago in late 2016.

22. On information and belief, Defendants’ failure to timely and properly notify Uber drivers and users in South Carolina of the security breach was a willful and knowing violation of South Carolina law.

23. On information and belief, Defendants’ failure to timely and properly notify Uber drivers and users in South Carolina of the security breach was a negligent violation of South Carolina law.

24. Plaintiff and other Uber drivers and users all suffered an injury in fact because they have suffered an increased risk of future identity theft as a result of the data breach and the failure to properly and timely notify victims of the security breach. Hackers are likely to use the victims’ personal identifying information for the fraudulent or criminal purposes in the future, including sale on the black market.

25. The personal identifying information of Plaintiff and other Uber drivers and users in South Carolina has intrinsic value to these persons and that value has been lost or negatively affected as a result of the data breach and the failure to properly and timely notify victims of the security breach. Such information has a market value in both legitimate markets, e.g., the use of such information by credit reporting agencies, and illegal black markets where it is sold and used for fraudulent or criminal purposes. The personal, private information of Plaintiff and other Uber

drivers and users is highly valuable to them as well as to identity thieves who desire to use the information for fraudulent or criminal purposes.

26. Fees paid by Plaintiff and other Uber drivers and users in South Carolina are paid, in part, to Defendants to ensure that personal identifying information is properly safeguarded and protected by Defendants.

27. As a result of Defendants' willful and knowing, or negligent, violation of South Carolina law, Uber drivers and users in South Carolina were deprived of the ability for more than a year to take actions to protect their identity, including, but not limited to, placing a fraud alert on their credit reporting accounts, placing a security freeze on their credit reporting accounts, more closely monitoring their credit reporting accounts, or taking other actions to protect their identity, personal, private information and livelihood.

28. As a result of Defendants' breach of their statutory duties, Plaintiff and class members have suffered and will continue in the future to suffer damages resulting from the data breach, including, but not limited to, mental anguish and emotional distress; physical pain and suffering, including loss of appetite and sleep; loss of enjoyment of life; increased risk of identity theft; credit monitoring expenses; damage to credit reports and ratings; and damages and expenses caused by the fraudulent theft and use of their identity, which may occur in connection with fraudulently opened credit accounts, fraudulently filed tax returns or fraudulent employment.

29. On information and belief, Defendants have offered to pay for credit monitoring for affected persons for an unspecified period, a remedy which is utterly inadequate given the fact that Plaintiff and class members have lost all or part of the intrinsic value of their personal identifying information and now have a significantly higher risk of becoming victims of identity theft, and that such thefts are most likely to occur after any free monitoring period ends.

CLASS ACTION ALLEGATIONS

30. Plaintiff incorporates each of the foregoing allegations as fully as if repeated herein verbatim.

31. Plaintiff brings this suit as a class action pursuant to Rule 23 of the South Carolina Rules of Civil Procedure, on behalf of himself and all other similarly situated persons as members of classes initially defined as:

- (1) All persons currently working or who previously worked as an Uber driver in South Carolina for the period of November 22, 2014, to the present whose personal identifying information was obtained from Defendants by unauthorized persons as a result of the security breach in late 2016; and
- (2) All persons currently using or who previously have used Uber services in South Carolina for transportation services for the period of November 22, 2014, to the present whose personal identifying information was obtained from Defendants by unauthorized persons as a result of the security breach in late 2016.

32. The classes as defined above are so numerous that joinder of all members is impracticable. Class members can be identified by records maintained by Defendants.

33. There are questions of law or fact common to the class. Common questions of law and fact include whether Defendants willfully or knowingly, or negligently, failed to timely and properly notify Plaintiff and class members about the security breach in late 2016; whether Defendants owed a duty to properly safeguard the personal identifying information of Plaintiff and the class members, and whether the duty was breached; whether the Plaintiff and the class members have suffered damages and are at increased risk of identity theft as a result of Defendants' wrongful actions or omissions; whether Plaintiff and the class members have lost all or part of the intrinsic value of their personal identifying information; whether Defendants' actions violated the South Carolina Consumer Protection Code; and whether Plaintiff and the class members are entitled to a declaratory judgment and injunctive relief.

34. The claims or defenses of the representative parties are typical of the claims or defenses of the class. Plaintiff's claims are typical of the claims of members of the Class because all suffered the same type of damages arising out of Defendants' wrongful conduct as described herein. Specifically, the claims of Plaintiff and class members arise from Defendants' failure to timely and properly notify Plaintiff and class members about the security breach in late 2016 and whether Defendants failed to properly safeguard the personal information of Plaintiff and class members.

35. The representative parties will fairly and adequately protect the interests of the class. Plaintiffs have retained counsel competent and experienced in class action lawsuits. Plaintiffs have no interests antagonistic or in conflict with those of class members and therefore are adequate representatives for class members.

36. The amount of damages in controversy for each member of the class exceeds \$100.00.

FIRST CAUSE OF ACTION
(VIOLATION OF S.C. CODE ANN. § 39-1-90)

37. Plaintiff incorporates each of the foregoing allegations as fully as if repeated herein verbatim.

38. Each Defendant is a "person" conducting business in the State of South Carolina as defined in S.C. Code Ann. § 39-1-90(A).

39. "Personal identifying information" is defined in S.C. Code Ann. § 39-1-90(D)(3) to include a person's Social Security number, driver's license number or state identification card number, financial account number, credit or debit card number in combination with a security, access code or password, and other numbers or information which may be used to access a persons' financial accounts. See also S.C. Code Ann. § 16-13-510(D) (similar definition).

40. At all times herein mentioned, Defendants owned or licensed computerized data or other data that included personal identifying information.

41. Under § 39-1-90(A), Defendants were required to disclose a breach of the security of its system and/or disclosure of personal identifying information “in the most expedient time possible and without unreasonable delay.”

42. Upon the breach of its own security procedures which, upon information and belief, first occurred in late 2016 by Defendants’ own admission, Defendants were required to halt the removal of the information, take remedial measures, and timely and properly notify all persons whose information was affected.

43. On information and belief, Defendants made no effort to notify and did not notify Plaintiff or any of its drivers and users about the security breach, which it admits occurred in late 2016, until November 21, 2017.

44. On information and belief, Defendants’ failure to timely and properly notify Uber drivers and users in South Carolina of the security breach was a willful and knowing violation of South Carolina law.

45. On information and belief, Defendants’ failure to timely and properly notify Uber drivers and users in South Carolina of the security breach was a negligent violation of South Carolina law.

46. On information and belief, Defendants waited for about one year before providing notice of any kind at all to Plaintiff and other Uber drivers and users in South Carolina, and Defendants have failed to comply with S.C. Code Ann. § 39-1-90(E).

47. As a result of Defendants’ willful and knowing, or negligent, violation of South Carolina law, Uber drivers and users in South Carolina were deprived of the ability for more than

a year to take actions to protect their identity, including, but not limited to, placing a fraud alert on their credit reporting accounts, placing a security freeze on their credit reporting accounts, more closely monitoring their credit reporting accounts, or taking other actions to protect their identity, personal, private information and livelihood.

48. As a result of Defendants' breach of these statutes, Plaintiff and class members have suffered and will continue in the future to suffer damages resulting from the data breach, including, but not limited to, mental anguish and emotional distress; physical pain and suffering, including loss of appetite and sleep; loss of enjoyment of life; increased risk of identity theft; credit monitoring expenses; damage to credit reports and ratings; and damages and expenses caused by the fraudulent theft and use of their identity, which may occur in connection with fraudulently opened credit accounts, fraudulently filed tax returns or fraudulent employment.

49. As a direct and proximate result of the foregoing breach of its notification and remedial duties, and pursuant to S.C. Code Ann. § 39-1-90(G), Plaintiff and class members are entitled to:

- a. institute a civil action to recover damages in case of a willful and knowing violation;
- b. institute a civil action that must be limited to actual damages resulting from a violation in case of a negligent violation of this section;
- c. seek an injunction to enforce compliance; and
- d. recover attorney's fees and court costs, if successful.

50. Additionally, Defendants are liable for such civil fines, administrative penalties and other sanctions provided under S.C. Code Ann. § 39-1-90(H); see also S.C. Code Ann. § 1-11-490 (containing similar provisions with regard to state agencies).

SECOND CAUSE OF ACTION
(CIVIL CONSPIRACY)

51. Plaintiffs incorporate each of the foregoing allegations as fully as if repeated herein verbatim.

52. Defendants owe a duty to Plaintiff and the class members to timely and properly notify them of security breaches as required by South Carolina law.

53. Defendants owe a duty to Plaintiff and the class members to safeguard and adequately protect their personal information.

54. Defendants' employees and agents, at all relevant times, acted within the course and scope of their employment by Defendants.

55. Defendants are vicariously liable for the actions and omissions of their employees and agents.

56. On information and belief, Travis Kalanick, Defendants' co-founder and former chief executive, became aware of the breach a month after it occurred. Instead of reporting the attack to regulators and victims last year, Defendants paid hackers \$100,000 to delete the data and keep the security breach under wraps.

57. On information and belief, the security breach resulted in the theft of personal identifying information held by Defendants about their drivers and users in South Carolina.

58. On information and belief, Defendants asserted and admitted that they never notified any Uber driver or user about the security breach until November 21, 2017, even though it occurred about one year ago.

59. Defendants engaged in a civil conspiracy with other, unknown persons, in a combination of two or more persons or legal entities, to conceal the security breach from Uber drivers and users in South Carolina.

60. Defendants engaged in a civil conspiracy for the purpose of injuring Plaintiff and class members, and which caused special damages to Plaintiff.

61. As a result of Defendants' willful and knowing, or negligent, violation of South Carolina law, Uber drivers and users in South Carolina were deprived of the ability for more than a year to take actions to protect their identity, including, but not limited to, placing a fraud alert on their credit reporting accounts, placing a security freeze on their credit reporting accounts, more closely monitoring their credit reporting accounts, or taking other actions to protect their identity, personal, private information and livelihood.

62. As a result of Defendants' breach of their statutory duties, Plaintiff and class members have suffered and will continue in the future to suffer damages resulting from the data breach, including, but not limited to, mental anguish and emotional distress; physical pain and suffering, including loss of appetite and sleep; loss of enjoyment of life; increased risk of identity theft; credit monitoring expenses; damage to credit reports and ratings; and damages and expenses caused by the fraudulent theft and use of their identity, which may occur in connection with fraudulently opened credit accounts, fraudulently filed tax returns or fraudulent employment.

THIRD CAUSE OF ACTION
**(NEGLIGENCE, GROSS NEGLIGENCE, RECKLESSNESS, NEGLIGENT HIRING,
NEGLIGENT TRAINING AND NEGLIGENT SUPERVISION)**

63. Defendants owe a duty to Plaintiff and the class members to timely and properly notify them of security breaches as required by South Carolina law.

64. Defendants owe a duty to Plaintiff and the class members to safeguard and adequately protect their personal information.

65. Defendants' employees and agents, at all relevant times, acted within the course and scope of their employment by Defendants.

66. Defendants are vicariously liable for the actions and omissions of their employees and agents.

67. “Personal information,” as defined in S.C. Code Ann. § 30-2-30(1) of the S.C. Family Privacy Protection Act and as used in this lawsuit, includes, but is not limited to, “information that identifies or describes an individual including, but not limited to, an individual’s photograph or digitized image, social security number, date of birth, driver’s identification number, name, home address, home telephone number, medical or disability information, education level, financial status, bank account numbers, account or identification number issued by or used, or both, by any federal or state governmental agency or private financial institution, employment history, height, weight, race, other physical details, signature, biometric identifiers, and any credit records or reports.”

68. The South Carolina Legislature, in establishing limitations on the collection and use of social security numbers by state and local governments in the S.C. Family Privacy Protection Act, has found that “[t]he social security number can be used as a tool to perpetuate fraud against an individual and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to the individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes and other legitimate consensual purposes. . . . When state and local government entities possess social security numbers or other personal identifying information, the governments should minimize the instances this information is disseminated either internally within government or externally with the general public.” S.C. Code Ann. § 30-2-300.

69. “Personal identifying information” is defined in S.C. Code Ann. § 39-1-90(D)(3) to include a person’s Social Security number, driver’s license number or state identification card number, financial account number, credit or debit card number in combination with a security, access code or password, and other numbers or information which may be used to access a persons’ financial accounts. See also S.C. Code Ann. § 16-13-510(D) (similar definition).

70. The Federal Trade Commission (“FTC”) has issued a publication entitled “Protecting Personal Information: A Guide for Business” (“FTC Report”).¹ In this publication, the FTC provides guidelines for businesses on how to develop a “sound data security plan” to protect against crimes of identity theft. To protect the personal sensitive information in their files, the FTC Report instructs businesses on following guidelines, among others:

- a) Restrict the use of portable storage devices such as laptops, external hard drives and flash or USB drives to those employees who need them to perform their jobs;
- b) Consider whether sensitive information really needs to be stored on a portable storage device such as a laptop or external hard drive;
- c) Require employees to store portable storage devices in a secure place;
- d) Consider allowing users of portable storage devices such as laptops to only access sensitive information, but not to store the information on the device. The information may be further protected by the use of a token, “smart card,” thumb print, or other biometric – as well as a password – to access the central computer;
- e) If a portable storage device contains sensitive data, encrypt it and configure it so users cannot download any software or change the security settings without approval from

¹ The FTC Report is available at <http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business>.

IT specialists. Consider adding an “auto-destroy” function so that data on a computer that is reported stolen will be destroyed when the thief uses it to try to get on the Internet;

f) Keep an inventory of all computers, laptops and portable storage devices where the company stores sensitive data;

g) Do not collect personal information if there is no legitimate business need. If there is a legitimate business need, only keep the information as long as necessary;

h) Use social security numbers only for required and lawful purposes and do not store these numbers unnecessarily, such as for an employee or customer identification number;

i) Encrypt personal information, particularly if the sensitive information is shipped to outside carriers or contractors;

j) Do not store sensitive computer data on any computer with an Internet connection unless it is essential for conducting the business;

k) Control access to sensitive information by requiring that employees use “strong” passwords; tech security experts believe the longer the password, the better;

l) Implement information disposal practices reasonable and appropriate to prevent unauthorized access to personal information;

m) Ask every new employee to sign an agreement to follow the company’s confidentiality and security standards for handling sensitive data. Make sure they understand that abiding by the company’s data security plan is an essential part of their duties. Regularly remind employees of the company’s policy and any legal requirement to keep personal information secure and confidential.

- n) Know which employees have access to consumers' sensitive personally identifying information. Pay particular attention to data like Social Security numbers and account numbers. Limit access to personal information to employees with a "need to know";
- o) Have a procedure in place for making sure that workers who leave employment or transfer to another part of the company no longer have access to sensitive information. Terminate their passwords, and collect keys and identification cards as part of the check-out process. Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate. Make sure the company's policies cover employees who telecommute or access sensitive data from home or an offsite location.
- p) Require employees to notify management immediately if there is a potential security breach, such as a lost or stolen laptop; and
- q) Impose disciplinary measures for security policy violations.

71. In a 2012 report titled "Identity Theft: Total Extent of Refund Fraud Using Stolen Identities is Unknown,"² the United States Government Accountability Office noted that the Internal Revenue Service reported more than 1,078,000 incidents of identity theft in connection with tax returns in 2012. The report states that the IRS's ability to detect such fraud is limited and the number of incidents which go undetected is unknown. The report states that "[t]he full extent and nature of identity theft-based refund fraud is not known, but IRS data indicate that it is a large and growing problem. The data show that in the first 9 months of 2012, the number of known tax-

² The 2012 GAO report is available at <http://www.gao.gov/products/GAO-13-132T>.

related identity theft incidents has already more than doubled over 2011.” The report states that “identity theft imposes a financial and emotional toll on its victims.”

72. In a 2007 report titled “Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown,”³ the GAO states that “[i]dentity theft occurs when individuals’ identifying information is used without authorization in an attempt to commit fraud or other crimes. There are two primary forms of identity theft. First, identity thieves can use financial account identifiers, such as credit card or bank account numbers, to take over an individual’s existing accounts to make unauthorized charges or withdraw money. Second, thieves can use identifying data, which can include such things as SSNs and driver’s license numbers, to open new financial accounts and incur charges and credit in an individual’s name, without that person’s knowledge. This second form of identity theft is potentially the most damaging because, among other things, it can take some time before a victim becomes aware of the problem, and it can cause substantial harm to the victim’s credit rating. While some identity theft victims can resolve their problems quickly, others face substantial costs and inconvenience repairing damage to their credit records. According to FTC, millions of Americans have their identities stolen each year. Roughly 85 percent of these cases involve the misuse of existing accounts and 35 percent involve new account creation or other fraud. (Twenty percent of the total involve both.)”

73. In the 2007 report, the GAO states that “[n]o single federal law enforcement agency has primary jurisdiction over identity theft crimes. Identity theft is not typically a stand-alone crime but rather a component of one or more crimes such as bank fraud, credit card fraud, social program

³ The 2007 GAO report is available at <http://www.gao.gov/products/GAO-07-737>.

fraud, tax refund fraud, and mail fraud. For example, a fraudster might steal another individual's personal identifying information in one city and use the information to commit credit card fraud and mail fraud in another city or state." As the GAO notes, this type of identity theft is the most damaging because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim's credit rating.

74. In the 2007 report, the GAO states that more than 570 breaches involving theft of personal identifiers such as social security numbers were reported by the news media from January 2005 through January 2006. These data breaches involve the "unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers."

75. Data breaches can lead to identity theft. As the GAO reported, "identity theft" is a broad term encompassing various types of criminal activities. Generally, identity theft occurs when a person's identifying information is used to commit fraud or other crimes. These crimes include credit card fraud, phone or utilities fraud, bank fraud, and government fraud. The FTC has stated that identity theft has been a serious problem in recent years, with approximately 9 million Americans as the victims of identity theft each year.

76. The GAO report states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

77. The release of social security numbers is particularly damaging because identity thieves are able to not only fraudulently open credit card accounts and to obtain loans, but also to fraudulently access consumers' existing accounts. Social security numbers, however, cannot be easily changed like a credit card account number. If an individual's social security number has

been compromised, it is much more difficult to protect against identity theft than it would be if credit card information were stolen. Even if an individual overcomes the barriers to changing the social security number, the defensive measure is still not a guarantee of protection against identity theft. Moreover, identity theft crimes often encompass more than just immediate financial loss. Identity thieves often hold onto stolen personal and financial information for several years before using or selling the information to other identity thieves.

78. In a 2012 report identifying the most serious problems faced by the IRS, the National Taxpayer Advocate Service states that an identity thief not only may file bogus tax returns and claim a taxpayer's refund, but also may gain employment under false pretenses.⁴ The report explains that "[i]n both situations, the victim is often sent on a journey through IRS processes and procedures that may take years to complete."

79. In 2009 and 2012 reports comparing the risk of identity theft among Data Breach Victims with the risk to the general population, Javelin Strategy & Research found that 20% of Data Breach Victims would ultimately become Identity Theft Victims, compared to 4% of the population generally. Thus, Data Breach Victims are significantly more likely to become Identity Theft Victims.⁵

80. Defendants were aware or reasonably should have been aware of a standard or "best practice" in the industry when it came to protecting the private information of employees, given

⁴ The NTAS report is available at <https://taxpayeradvocate.irs.gov/2012-Annual-Report/downloads/Most-Serious-Problems-Identity-Theft.pdf>.

⁵ Source: Javelin Strategy & Research, Data Breach Notifications: Victims Face Four Times Higher Risk of Fraud (October 2009) at 4, available at <http://www.javelinstrategy.com>. See also, Javelin 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters. <https://www.javelinstrategy.com/brochure/276>

the considerable news coverage as well as the focus of the business community and government on similar data breaches in recent years.

81. On information and belief, Defendants breached their duty to Plaintiff and class members in one or more of the following ways by causing, allowing or enabling the theft of personal, private information:

- a. In failing to take adequate and reasonable security measures to properly safeguard the personal information of Plaintiff and the class members;
- b. In failing to establish or enforce reasonable and appropriate business practices regarding the safekeeping of the personal information Plaintiff and the class members;
- c. In failing to properly encrypt the personal information of Plaintiff and class members;
- d. In negligently hiring one or more employees who allowed or caused a data breach to occur;
- e. In negligently training one or more employees who allowed or caused a data breach to occur;
- f. In negligently supervising one or more employees who allowed or caused a data breach to occur;
- g. In failing to establish or enforce additional security precautions, policies or procedures in order to ensure that personal information of Plaintiff and class members;
- h. In failing to take adequate measures following discovery of the breach, including the failure to provide credit monitoring off sufficient duration; and

i. In other ways which will be discovered during the course of this case.

82. The breach by Defendants of one or more of these various duties was the sole or concurrent proximate cause of damages suffered by Plaintiff and class members.

83. As a result of Defendants' willful and knowing failure to timely and properly notify Uber drivers and users about the security breach in late 2016, Plaintiff and class members in South Carolina were deprived of the ability for more than a year to take actions to protect their identity, including, but not limited to, placing a fraud alert on their credit reporting accounts, placing a security freeze on their credit reporting accounts, more closely monitoring their credit reporting accounts, or taking other actions to protect their identity, personal, private information and livelihood.

84. As a result of Defendants' negligent or wrongful acts or omissions, Plaintiff and class members have suffered and will continue in the future to suffer damages resulting from the data breach, including, but not limited to, mental anguish and emotional distress; physical pain and suffering, including loss of appetite and sleep; loss of enjoyment of life; increased risk of identity theft; credit monitoring expenses; damage to credit reports and ratings; and damages and expenses caused by the fraudulent theft and use of their identity, which may occur in connection with fraudulently opened credit accounts, fraudulently filed tax returns or fraudulent employment.

85. Plaintiffs and class members are entitled to recover actual, special and consequential damages from Defendants in an amount to be determined by a jury of their peers. Further, Plaintiff and class members are entitled to recover punitive damages from Defendants for their wrongful, grossly negligent, willful, wanton and reckless actions in an amount to be determined by a jury.

FOURTH CAUSE OF ACTION
**(BREACH OF EXPRESS OR IMPLIED CONTRACT AND BREACH OF COVENANTS
OF GOOD FAITH AND FAIR DEALING BY PLAINTIFF AND CLASS MEMBERS
WHO ARE OR WERE UBER DRIVERS)**

86. Plaintiff incorporates each of the foregoing allegations as fully as if repeated herein verbatim.

87. Defendants entered into an at-will contract of employment or agency with Plaintiff and class members who currently work or previously have worked as Uber drivers. Defendants offered employment or work as an Uber driver, which Plaintiff and members of the Class accepted, and the parties exchanged mutual consideration.

88. As part of the express or implied employment or agency contract, Plaintiff and Uber drivers were required by Defendant to undergo a background check and screening process and must provide, among other things, their name, address, email address, telephone number, driver's license, Social Security number, financial account information, vehicle registration, proof of insurance, proof of vehicle inspection and must have a vehicle meeting specified requirements.

89. As part of the express or implied employment or agency contract, Plaintiff and Uber drivers understood and expected that Defendants would properly safeguard their personal, private information and adequately protect it from theft by unauthorized persons or use for improper, fraudulent or criminal purposes.

90. Fees paid by Plaintiff and other Uber drivers and users in South Carolina are paid, in part, to Defendants to ensure that personal identifying information is properly safeguarded and protected by Defendants.

91. Defendants breached the express or implied contract with Plaintiff and class members by failing to properly safeguard their personal identifying information as described herein.

92. By their actions, Defendants violated the covenants of good faith and fair dealing that are implicit in every contract.

93. As a result of Defendants' breach of contract and of the covenants of good faith and fair dealing, and failure to timely and properly notify Uber drivers and users about the security breach in late 2016, Plaintiff and class members in South Carolina were deprived of the ability for more than a year to take actions to protect their identity, including, but not limited to, placing a fraud alert on their credit reporting accounts, placing a security freeze on their credit reporting accounts, more closely monitoring their credit reporting accounts, or taking other actions to protect their identity, personal, private information and livelihood.

94. As a result of Defendants' breach of contract and of the covenants of good faith and fair dealing, Plaintiff and class members have suffered and will continue in the future to suffer damages resulting from the data breach, including, but not limited to, mental anguish and emotional distress; physical pain and suffering, including loss of appetite and sleep; loss of enjoyment of life; increased risk of identity theft; credit monitoring expenses; damage to credit reports and ratings; and damages and expenses caused by the fraudulent theft and use of their identity, which may occur in connection with fraudulently opened credit accounts, fraudulently filed tax returns or fraudulent employment.

95. Plaintiff and class members are entitled to recover actual, special and consequential damages from Defendant in an amount to be determined by a jury of their peers.

FIFTH CAUSE OF ACTION
**(BREACH OF EXPRESS OR IMPLIED CONTRACT AND BREACH OF COVENANTS
OF GOOD FAITH AND FAIR DEALING BY PLAINTIFF AND CLASS MEMBERS
WHO ARE OR WERE UBER USERS)**

96. Plaintiff incorporates each of the foregoing allegations as fully as if repeated herein verbatim.

97. Defendants entered into an express or implied contract to provide a communication or transportation service with Plaintiff and class members who are or were Uber users. Defendants offered its services, which Plaintiff and class members accepted, and the parties exchanged mutual consideration.

98. As part of the express or implied contract, Plaintiff and Uber users were required by Defendants to provide personal information, including, but not limited to, their names, addresses, email addresses and financial account numbers.

99. As part of the express or implied contract and as required by law, Plaintiff and class members understood and expected that Defendants would properly safeguard their personal information and adequately protect it from theft by unauthorized persons or use for improper or unlawful purposes.

100. Fees paid by Plaintiff and other Uber drivers and users in South Carolina are paid, in part, to Defendants to ensure that personal identifying information is properly safeguarded and protected by Defendants.

101. Defendants breached the express or implied contract with Plaintiff and class members by failing to properly safeguard their personal information as described herein.

102. By their actions, Defendants violated the covenants of good faith and fair dealing that are implicit in every contract.

103. As a result of Defendants' breach of contract and of the covenants of good faith and fair dealing, and failure to timely and properly notify Uber drivers and users about the security breach in late 2016, Plaintiff and class members in South Carolina were deprived of the ability for more than a year to take actions to protect their identity, including, but not limited to, placing a fraud alert on their credit reporting accounts, placing a security freeze on their credit reporting

accounts, more closely monitoring their credit reporting accounts, or taking other actions to protect their identity, personal, private information and livelihood.

104. As a result of Defendants' breach of contract and of the covenants of good faith and fair dealing, Plaintiff and class members have suffered and will continue in the future to suffer damages resulting from the data breach, including, but not limited to, mental anguish and emotional distress; physical pain and suffering, including loss of appetite and sleep; loss of enjoyment of life; increased risk of identity theft; credit monitoring expenses; damage to credit reports and ratings; and damages and expenses caused by the fraudulent theft and use of their identity, which may occur in connection with fraudulently opened credit accounts, fraudulently filed tax returns or fraudulent employment.

105. Plaintiffs and class members are entitled to recover actual, special and consequential damages from Defendants in an amount to be determined by a jury of their peers.

SIXTH CAUSE OF ACTION
(VIOLATION OF CONSUMER IDENTITY THEFT PROTECTION ACT)

106. Plaintiff incorporates each of the foregoing allegations as fully as if repeated herein verbatim.

107. Defendants' employees and agents, at all relevant times, acted within the course and scope of their employment by Defendants.

108. Defendants are vicariously liable for the actions and omissions of its employees and agents.

109. Plaintiffs and class members possess and enjoy legal rights pursuant to the Consumer Identity Theft Protection provisions contained in the South Carolina Consumer Protection Code, S.C. Code Ann. § 37-20-110 et seq.

110. Each Defendant is a “person” or “organization” as defined in the Consumer Protection Code. S.C. Code Ann. § 37-20-110(10) and § 37-1-301(18) and (20).

111. Defendants possessed and required Plaintiff and class members to submit “personal identifying information” as a condition of employment or agency, or working as an Uber driver or using Uber services. S.C. Code Ann. § 37-20-110(11)(a) and § 16-3-510(D).

112. A “security breach” occurred as a result of Defendants’ knowing, willful, negligent or wrongful actions or omissions, as described herein. S.C. Code Ann. § 37-20-110(15).

113. As a result of Defendants’ knowing, willful or negligent violations, the personal identifying information of Plaintiff and class members was not adequately protected from theft by unauthorized persons or use for improper or unlawful purposes, and now or in the future may be publicly posted or displayed in violation of the law. S.C. Code Ann. §§ 37-20-110(13) and 37-20-180.

114. As a result of Defendants’ knowing or willful violations, Plaintiff and class members each are entitled to recover three times the amount of actual damages or three thousand dollars for each incident, whichever is greater, as well as reasonable attorney’s fees and costs. S.C. Code Ann. § 37-20-170(D).

115. As a result of Defendants’ negligent violations, Plaintiff and class members each are entitled to recover the greater of actual damages or one thousand dollars for each incident, as well as reasonable attorney’s fees and costs. S.C. Code Ann. § 37-20-170(E).

116. As a result of Defendants’ breach of these statutes and failure to timely and properly notify Uber drivers and users about the security breach in late 2016, Plaintiff and class members in South Carolina were deprived of the ability for more than a year to take actions to protect their identity, including, but not limited to, placing a fraud alert on their credit reporting accounts,

placing a security freeze on their credit reporting accounts, more closely monitoring their credit reporting accounts, or taking other actions to protect their identity, personal, private information and livelihood.

117. As a result of Defendants' breach of these statutes, Plaintiff and class members have suffered and will continue in the future to suffer damages resulting from the data breach, including, but not limited to, mental anguish and emotional distress; physical pain and suffering, including loss of appetite and sleep; loss of enjoyment of life; increased risk of identity theft; credit monitoring expenses; damage to credit reports and ratings; and damages and expenses caused by the fraudulent theft and use of their identity, which may occur in connection with fraudulently opened credit accounts, fraudulently filed tax returns or fraudulent employment.

118. Plaintiff and class members are entitled to recover actual, special and consequential damages from Defendants in an amount to be determined by a jury of their peers. Plaintiff and class members are entitled to recover punitive damages from Defendants for its wrongful, grossly negligent, willful, wanton and reckless actions in an amount to be determined by a jury.

SEVENTH CAUSE OF ACTION
(DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF)

119. Plaintiff incorporates each of the foregoing allegations as fully as if repeated herein verbatim.

120. Pursuant to the Uniform Declaratory Judgments Act, S.C. Code Ann. § 15-53-10 et seq., Plaintiff asks the Court to declare:

- a. That Defendants by their failure to timely and properly notify Uber drivers and users about the security breach in late 2016, Plaintiff and class members in South Carolina were deprived of the ability for more than a year to take actions to protect their identity, including, but not limited to, placing a fraud alert on

their credit reporting accounts, placing a security freeze on their credit reporting accounts, more closely monitoring their credit reporting accounts, or taking other actions to protect their identity and livelihood; that Plaintiff and class members are entitled to recover past, present and future damages as a result thereof, including statutory damages and attorney's fees and costs pursuant to S.C. Code Ann. § 39-1-90(G) and (H);

- b. That Defendants by their negligent, grossly negligent, reckless, knowing, willful or wrongful acts, as described herein, was negligent, grossly negligent or reckless in failing to timely and properly notify Uber drivers and users about the security breach in late 2016, and that Plaintiff and class members are entitled to recover their past, present and future damages;
- c. That Defendants by their negligent, grossly negligent, reckless, knowing, willful, or wrongful acts, as described herein, breached an express or implied contract with Plaintiff and class members and violated the covenants of good faith and fair dealing, and that Plaintiff and class members are entitled to recover their past, present and future damages;
- d. That Defendants by their negligent, knowing, willful or wrongful acts, as described herein, violated the Consumer Identity Theft Protection Act (S.C. Code Ann. § 37-20-110 et seq.), and that Plaintiff and class members are entitled to recover penalties and their past, present and future damages, and attorney's fees and costs; and

- e. That Plaintiff and class members entitled to temporary and permanent injunctive relief requiring Defendants to take appropriate action to safeguard and adequately protect the personal information of Plaintiff and class members.

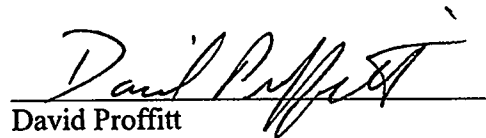
DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all causes of action to which they are entitled by law to a trial by a jury of their peers.

WHEREFORE, having fully set forth their Complaint, Plaintiff prays that the Court grant by verdict or judgment against Defendants an award of all damages they are entitled to recover under the law under all causes of action set forth in this Complaint, including actual damages, consequential damages, special damages, penalties and punitive damages in an amount to be determined by a jury, and declaratory and injunctive relief, including attorney's fees and costs as allowed by any statute or court rule, and such other and further relief as the Court may deem just and proper.

Respectfully submitted,

PROFFITT & COX, LLP



David Proffitt
SC Bar No. 11193
Ronald B. Cox
SC Bar No. 11129
140 Wildewood Park Drive, Suite A
Columbia, S.C. 29223
Telephone: (803) 834-7097
Fax: (888) 711-1057
dproffitt@proffittcox.com
rcox@proffittcox.com

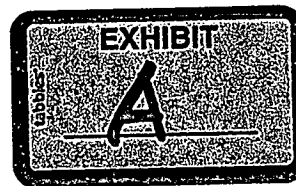
Attorneys for Plaintiffs

November 22, 2017



US -- Nov 21, 2017

2016 Data Security Incident



Written by Dara Khosrowshahi, CEO

Share

As Uber’s CEO, it’s my job to set our course for the future, which begins with building a company that every Uber employee, partner and customer can be proud of. For that to happen, we have to be honest and transparent as we work to repair our past mistakes.

I recently learned that in late 2016 we became aware that two individuals outside the company had inappropriately accessed user data stored on a third-party cloud-based service that we use. The incident did not breach our corporate systems or infrastructure.

Our outside forensics experts have not seen any indication that trip location history, credit card numbers, bank account numbers, Social Security numbers or dates of birth were downloaded. However, the

11/22/2017

2016 Data Security Incident | Uber Newsroom

- The names and driver's license numbers of around 600,000 drivers in the United States. Drivers can learn more here.
- Some personal information of 57 million Uber users around the world, including the drivers described above. This information included names, email addresses and mobile phone numbers. Riders can learn more here.

At the time of the incident, we took immediate steps to secure the data and shut down further unauthorized access by the individuals. We subsequently identified the individuals and obtained assurances that the downloaded data had been destroyed. We also implemented security measures to restrict access to and strengthen controls on our cloud-based storage accounts.

You may be asking why we are just talking about this now, a year later. I had the same question, so I immediately asked for a thorough investigation of what happened and how we handled it. What I learned, particularly around our failure to notify affected individuals or regulators last year, has prompted me to take several actions:

- I've asked Matt Olsen, a co-founder of a cybersecurity consulting firm and former general counsel of the National Security Agency and director of the National Counterterrorism Center, to help me think

11/22/2017

2016 Data Security Incident | Uber Newsroom

led the response to this incident are no longer with the company.

- We are individually notifying the drivers whose driver's license numbers were downloaded.
- We are providing these drivers with free credit monitoring and identity theft protection.
- We are notifying regulatory authorities.
- While we have not seen evidence of fraud or misuse tied to the incident, we are monitoring the affected accounts and have flagged them for additional fraud protection.

None of this should have happened, and I will not make excuses for it. While I can't erase the past, I can commit on behalf of every Uber employee that we will learn from our mistakes. We are changing the way we do business, putting integrity at the core of every decision we make and working hard to earn the trust of our customers.

Share this post



ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Uber Sued on Behalf of South Carolina Drivers, Riders Whose Data Was Stolen in 2016 Breach](#)
