Patrice L. Bishop (182256)
pbishop@ssbla.com
STULL, STULL & BRODY
9430 W. Olympic Blvd., Suite 400
Beverly Hills, CA 90212
Tel: 310-209-2468
Fax: 310-209-2087

Counsel for Plaintiffs

(Additional Counsel on Signature Page)

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

BENJAMIN HELLER, DAVID FLUSS, ANNA LUNA, MARCY LOKIETZ, AKASH SHETH, Individually and on Behalf of all Others Similarly Situated,

Plaintiffs,

v.

RASIER, LLC, RASIER-CA, LLC, and UBER TECHNOLOGIES, INC.,

Defendants.

Case No. 17-cv-8545

COMPLAINT

CLASS ACTION

DEMAND FOR JURY TRIAL

Plaintiffs Benjamin Heller, Anna Luna, David Fluss, Marcy Lokietz and Akash Sheth ("Plaintiffs"), by and through their undersigned counsel, submits this Complaint on behalf of themselves and all others similarly situated. Plaintiffs' allegations are based upon their personal knowledge as to themselves and their own acts, and upon information and belief, developed from the investigation and analysis by Plaintiffs' counsel, including a review of publicly available information.

NATURE OF THE ACTION

1. Plaintiffs bring this class action case against Rasier, LLC., Rasier-CA, LLC., Uber Technologies, Inc. (collectively referred to as either "Uber" or "Defendants") for their failure to secure and safeguard riders' and drivers' personally identifiable information ("PII") which Uber collected in connection with the operation of its business.

2. On November 21, 2017, Uber disclosed that in October 2016 hackers had stolen 57 million driver and rider accounts (the "Data Breach" or "Breach") and that Defendants had kept the data breach secret for more than a year after paying a $100,000 ransom.

3. Uber has acknowledged that a cybersecurity incident occurred, resulting in the theft of its riders' and drivers' PII, consisting of names, addresses, email addresses, credit card numbers and other information.

4. PII for Plaintiffs and the class of riders and drivers they seek to represent was compromised due to Uber's acts and omissions and their failure to properly protect PII.

5. Uber could have prevented this Data Breach.

6. Uber disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its riders and drivers the material fact that it did not have adequate security practices

to safeguard PII, failing to take available steps to prevent and stop the breach from ever happening, and failing to monitor and detect the breach on a timely basis.

7. As a result of the Data Breach, PII of the Plaintiffs and Class members has been exposed, in all likelihood, to criminals for misuse. The injuries suffered by Plaintiffs and Class members, or likely to be suffered as a direct result of the Data Breach, include:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, the costs of purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs and Class members' information on the Internet black market;

h. damages to and diminution in value of their PII entrusted to Uber for

the sole purpose of purchasing products and services from Uber; and

i. the loss of Plaintiffs' and Class members' privacy.

8. The injuries to the Plaintiffs and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for PII.

9. Further, Plaintiffs retain a significant interest in ensuring that their PII, which, while stolen, remains in the possession of Defendants, is protected from further breaches, and seeks to remedy the harms they have suffered on behalf of themselves and similarly situated riders and drivers whose PII was stolen as a result of the Data Breach.

10. Plaintiffs bring this action to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiffs seek the following remedies, among others: statutory damages under state and/or federal laws, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Defendants to implement improved data security measures.

PARTIES

11. Plaintiff Anna Luna is a California citizen residing in Encino, California, and was an Uber rider in October 2016.

12. Plaintiff Benjamin Heller is a New York citizen residing in New York, New York, and was an Uber rider in October 2016.

13. Plaintiff David Fluss is a Florida citizen residing in Tamarac, Florida, and was an Uber driver in October 2016.

14. Plaintiff Marcy Lokietz is a Florida citizen residing in Parkland, Florida, and was an Uber rider in October 2016.

15. Plaintiff Akash Sheth is a New Jersey citizen residing in Edison, New Jersey, and was an Uber driver in October 2016.

16. Defendant Rasier, LLC is a Limited Liability Company with its headquarters and principle place of business in San Francisco, California.

17. Defendants Rasier-CA, LLC is a Limited Liability Company with its headquarters and principle place of business in San Francisco, California.

18. Defendants Uber Technologies, Inc. is a corporation with its headquarters and principle place of business and corporate offices in San Francisco, California and is the parent company of Defendants Rasier and Rasier-CA.

19. The Defendants develop, market, and operate a ridesharing mobile application which allows consumers to submit a trip request, which is routed to crowd-sourced taxi drivers. Their smartphone application connects drivers with people who need a ride. Uber's application enables users to arrange and schedule transportation and/or logistics services with third party providers.

JURISDICTION AND VENUE

20. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2), because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiffs and Defendants are citizens of different states. The proposed Class and Sub-classes each include well over 100 members.

21. This Court has jurisdiction over Defendants because Uber regularly conducts business in California; and has sufficient minimum contacts in California. Defendants intentionally avail themselves of this jurisdiction by marketing and offering their services from California to millions of consumers nationwide, including Uber riders and drivers in the states of California, Florida, New York, and New Jersey.

22. Venue is proper in this District pursuant to 28 U.S.C. §1391 because Uber is registered to conduct business throughout California and regularly conducts business in this District.

CLASS ACTION ALLEGATIONS

23. Plaintiffs bring this class action pursuant to the Federal Rules of Civil Procedure 23(a) and (b)(3), on behalf of themselves and all others similarly situated in the United States, who were Uber riders and drivers during and since the Data Breach, had their personal information stolen from Uber's software application systems, and were damaged thereby (the "Class"). Plaintiffs also bring Counts on behalf of Sub-classes of California, New Jersey, New York and Florida residents who were Uber riders and drivers during and since the Data Breach and had their personal information stolen from Uber's software application systems and were damaged thereby (the "Sub-classes"). The Class and Sub-classes do not include Uber officers or directors.

24. The Class and Sub-classes consist of potentially millions of Uber riders and drivers. While the exact number of members of the Class and Sub-classes and the identities of individual members of the Class and Subclasses are unknown to Plaintiffs' counsel at this time, and can only be ascertained through appropriate discovery, based on the fact that 57 million Uber riders and drivers have been adversely affected, the membership of the Class and Sub-classes are each so numerous that joinder of all members is impracticable.

25. Uber's wrongful conduct affected all members of the Class and Sub-classes in exactly the same way. The Defendants' failure to properly safeguard its customer's personal information is completely uniform among the Class and Sub-classes.

26. Questions of law and fact common to all members of the Class and Sub-classes predominate over any questions affecting only individual members. Such common questions of law and fact include:

a. whether the Defendants acted wrongfully by failing to properly safeguard their riders' and drivers' personal information collected and stored by Uber on its software application system;

b. whether Defendants' conduct violated law;

c. whether the Plaintiffs and the other members of the Class and Subclasses have been damaged, and, if so, what is the appropriate relief; and

d. whether Defendants breached their duties owed to members of the Class and Subclasses and by failing to properly safeguard their personal information.

27. Plaintiffs' claims, as described herein, are typical of the claims of all other members of the Class and Sub-classes, as the claims of Plaintiffs and all other members of the Class and Sub-classes arise from the same set of facts regarding Defendants' failure to protect the Class and Sub-classes member's personal information from computer hackers. Plaintiffs maintain no interest antagonistic to the interests of other members of the Class or Sub-classes.

28. Plaintiffs are committed to the vigorous prosecution of this action and have retained competent counsel experienced in the prosecution of class actions of this type. Accordingly, Plaintiffs are adequate representatives of the Class and Sub-classes and will fairly and adequately protect their interests.

29. This class action is a fair and efficient method of adjudicating the claims of Plaintiffs and the Class and Sub-classes for the following reasons:

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

b. the prosecution of separate actions by individual Class and Sub-classes members would likely create a risk of inconsistent or varying adjudications with respect to individual members thereby establishing incompatible standards of conduct for Defendants or would allow some Class and Sub-classes members' claims to adversely affect the ability of other members to protect their interests;

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

d. Plaintiffs anticipates no difficulty in the management of this litigation as a class action; and

e. the Class and Sub-classes is readily definable, and prosecution as a class action will eliminate the possibility of repetitious litigation, while also providing redress for claims that may be too small to support the expense of individual, complex litigation.

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

SUBSTANTIVE ALLEGATIONS

31. Plaintiffs were riders with Uber and/or drivers for Uber prior to and during October 2016 and to the present, and provided Uber personal information in order to initiate their Uber account to be used solely by Uber for purposes of maintaining and facilitating such account.

32. On November 21, 2017, Uber announced that two hackers had stolen data about Uber's riders and drivers from a third-party server and then approached Uber and demanded payment of $100,000 to delete their copy of the data. Defendants discovered this breach as part of a larger investigation into Uber's business practices over a year ago.

33. Joe Sullivan, the Uber chief security officer at the time of the breach, who has since been fired, arranged the deal to pay the hackers the $100,000 in ransom. However, Uber did not stop at acquiescing to the hacker's demands and took it a step further. Uber successfully tracked down the hackers and forced them to sign nondisclosure agreements.

34. To further conceal the damage caused from this breach, Uber executives made it appear that rather than this payment being a ransom payoff, they

made the payoff appear to be part of a "bug bounty" which is a deal offered by many websites and software developers by which individuals can receive recognition and compensation for reporting "bugs" especially those pertaining to exploits and vulnerabilities in a company.

35. The failure to immediately or within a reasonable time report this data breach to relevant governmental agencies and to Uber users and drivers is a blatant and egregious violation of numerous state statutes specifically enacted to insure prompt disclosure of data breaches.

36. Furthermore, Plaintiffs and class members have suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their PII being placed in the hands of criminals who have already, or will imminently, misuse such information.

37. Moreover, Plaintiffs have a continuing interest in ensuring that their PII, which remains in the possession of Uber, is protected and safeguarded from future breaches.

38. At all relevant times, Uber was well-aware, or reasonably should have been aware, that the PII collected, maintained and stored by Uber is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

39. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches, Uber continued to use an outdated, insufficient and inadequate system to protect the PII of Plaintiffs and Class members.

40. PII is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers and other personal information on a number of underground Internet websites. It is common knowledge that PII is considered gold

to identity thieves because they can use victims' personal data to incur charges on existing accounts, or clone ATM, debit, or credit cards.

41. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[1]

42. At all relevant times, Uber knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

43. Uber was, or should have been, fully aware of the significant number of people whose PII it collected, and thus, the significant number of individuals who would be harmed by a breach of its system.

44. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, Uber's approach to maintaining the privacy and security of the PII of Plaintiffs and the Class members, and reporting any violation thereof in accordance with law, was lackadaisical, cavalier, reckless, or at the very least, negligent.

45. The ramifications of Uber's failure to keep Plaintiffs' and Class members' data secure are severe.

46. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[2] The FTC

---

[1] Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited Nov. 22, 2017).

[2] 17 C.F.R § 248.201 (2013).

describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[3]

47. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[4]

48. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[5]

49. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[6]

50. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before

---

[3] *Id.*

[4] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Nov. 22, 2017).

[5] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited Nov. 22, 2017).

[6] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Nov. 22, 2017).

> being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

51. Plaintiffs and the 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 use of their PII.

52. The PII of Plaintiffs and the Class members is private and sensitive in nature and was left inadequately protected by Uber.

53. The Data Breach was a direct and proximate result of Uber's failure to properly safeguard and protect Plaintiffs' and the Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Uber's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and the Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

54. Uber had the resources to prevent a breach, but neglected to timely and adequately invest in data security, despite the growing number of well-publicized data breaches.

55. Had Uber remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Uber would have prevented the Data Breach and, ultimately, the theft of its customers' PII.

---

[7] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited Nov. 22, 2017).

56. As a direct and proximate result of Uber's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and the Class members have been placed at an imminent, immediate, and continuing increased risk of fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives.

57. While the PII of Plaintiffs and members of the Class has been stolen, Uber continues to hold PII of consumers, including Plaintiffs and the Class members. Particularly because Uber and has demonstrated an inability to prevent a breach and immediately disclose it even after being detected, Plaintiffs and members of the Class have an undeniable interest in insuring that their PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

COUNT I

NEGLIGENCE

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE SUB-CLASSES)

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

59. Upon accepting and storing the PII of Plaintiffs and the Class Members in its computer systems and on its networks, Defendants undertook and owed a duty to Plaintiffs and the Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that PII was private and confidential and should be protected as private and confidential.

60. Defendants owed a duty of care not to subject Plaintiffs, along with their PII, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

61. Defendants owed numerous duties to Plaintiffs and to members of the Nationwide Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

62. Defendants also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks. Further, Defendants failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiffs and Class Members, misuse the PII and intentionally disclose it to others without consent.

63. Defendants knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Defendants knew about numerous, well-publicized data breaches.

64. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class Members' PII.

65. Defendants breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class Members.

66. Because Defendants knew that a breach of their systems would damage millions of individuals, including Plaintiffs and Class members, Defendants had a duty to adequately protect their data systems and the PII contained thereon.

67. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PII. Defendants' misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

68. Defendants also had independent duties under state and/or federal laws that required it to safeguard Plaintiffs' and Class members' PII.

69. Defendants breached their duties to Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class members' PII both before and after learning of the Data Breach; and

d. by failing to comply with the minimum industry data security standards during the period of the Data Breach.

70. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect PII of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiffs and Class members during the time it was within its possession or control.

71. Upon information and belief, Uber improperly and inadequately safeguarded PII of Plaintiffs and Class Members in deviation of standard industry

rules, regulations, and practices at the time of the unauthorized access. Defendants' failure to take proper security measures to protect sensitive PII of Plaintiffs and Class members, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiffs and Class members.

72. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiffs and Class members; and failing to provide Plaintiffs and Class members with timely and sufficient notice that their sensitive PII had been compromised.

73. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

74. As a direct and proximate result of the Defendant's conduct, Plaintiffs and the other members of the Class and Sub-Classes suffered damages including, but not limited to, loss of control of their PII, the burden and cost of heightened monitoring for signs for identity theft and for undertaking actions such as credit freezes and alerts to prevent identity theft, and remediating acts and damages caused by identity theft, and other economic damages.

COUNT II

NEGLIGENCE PER SE

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE SUB-CLASSES)

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

76. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or

practice by businesses, such as Uber, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

77. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

78. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

79. Plaintiffs and the Class Members are within the class of persons that the FTC Act was intended to protect.

80. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

81. As a direct and proximate result of the Defendant's conduct, Plaintiffs and the other members of the Class and Sub-Classes suffered damages including, but not limited to, loss of control of their PII, the burden and cost of heightened monitoring for signs for identity theft and for undertaking actions such as credit freezes and alerts to prevent identity theft, and remediating acts and damages caused by identity theft, and other economic damages.

///

///

///

COUNT III

BREACH OF IMPLIED CONTRACT

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE SUB-CLASSES)

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

83. By providing Plaintiffs' and the other Class and Sub-Classes members' PII to Uber as a rider or a driver, Plaintiffs and the other members of the Class and Sub-Classes entered into implied contracts with Uber pursuant to which Uber agreed to safeguard and protect such information from unauthorized access and theft.

84. Plaintiffs and the other members of the Class and Sub-Classes fully performed their obligations under the implied contracts with Uber.

85. Defendants breached the implied contracts it had made with the Plaintiffs and the other members of the Class and Sub-Classes by failing to safeguard and protect the personal and financial information of Plaintiffs and the other members of the Class and Sub-Classes, and by allowing unauthorized access to Uber's software application network and the mass exporting of PII from Uber.

86. The damages to Plaintiffs and the other members of the Class and Sub-Classes as described herein were the direct and proximate result of the Defendants' breaches of these implied contracts.

COUNT IV

DECLARATORY JUDGMENT

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE SUB-CLASSES)

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

88. As previously alleged, Plaintiffs and Class members entered into an implied contract that required Uber to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Uber owes duties of care to Plaintiffs and Class members that require it to adequately secure PII.

89. Uber still possesses PII pertaining to Plaintiffs and Class members.

90. Uber has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

91. Accordingly, Uber has not satisfied its contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Uber's lax approach towards data security has become public, the PII in its possession is more vulnerable than it previously was.

92. Actual harm has arisen in the wake of the Uber Data Breach regarding Uber's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class members.

93. Plaintiffs, therefore, seek a declaration that (a) Uber's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Uber must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Uber's systems on a periodic basis, and ordering Uber to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Uber is compromised, hackers cannot gain access to other portions of Uber systems;

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Uber customers must take to protect themselves.

COUNT V

VIOLATION OF FLORIDA'S UNFAIR TRADE PRACTICES ACT, FLA. STAT. § 501.201, *ET SEQ.*

(ON BEHALF OF PLAINTIFFS FLUSS AND LOKIETZ AND THE FLORIDA SUB-CLASS)

94. Plaintiffs Fluss and Lokietz incorporate and re-allege all allegations contained in the preceding paragraphs as if fully set forth herein.

95. At all relevant times, Florida Subclass members were "consumers" within the meaning of FDUPTA.

96. Uber is engaged in trade and commerce in Florida.

97. Plaintiffs Fluss and Lokietz and Class members entrusted Uber with their PII.

98. As alleged herein this Complaint, Uber engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the FDUTPA:

a. failure to maintain the security of credit Plaintiffs' PII;

b. failure to maintain adequate data security practices to safeguard Plaintiffs' PII;

b. failure to disclose that its data security practices were inadequate to safeguard Plaintiffs' PII from theft;

d. continued acceptance of PII and storage of other personal information after Uber knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach;

99. Uber knew or should have known that its data security practices were inadequate to safeguard the PII of Plaintiffs and the Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

100. As a direct and proximate result of Uber's violation of the FDUTPA, Plaintiffs Fluss and Lokietz and Class members suffered damages arising from the breach of their PII. The nature full nature of the damages and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

101. Also as a direct result of Uber's knowing violation of the FDUTPA, Plaintiffs Fluss and Lokietz and Class members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Uber engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Uber's systems on a periodic basis, and ordering Uber to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Uber engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Uber audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Uber segment PII by, among other things, creating firewalls and access controls so that if one area of Uber is compromised, hackers cannot gain access to other portions of Uber systems;

e. Ordering that Uber purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Uber conduct regular database scanning and securing checks;

g. Ordering that Uber routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Uber to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Uber customers must take to protect themselves.

102. Plaintiffs Fluss and Lokietz bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs Fluss and Lokietz and Class members and the public from Uber's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Uber's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

103. Plaintiffs Fluss and Lokietz and the Florida Sub-class seek actual damages under Fla. Stat. § 501.211 (2) and all fees, costs, and expenses allowed by law, including attorney's fees and costs, pursuant to Federal Rule of Civil Procedure 23 and Fla. Stat. §§ 501.2105 and 501.211, to be proven at trial.

COUNT VI

VIOLATION OF NEW JERSEY'S CONSUMER FRAUD ACT, N.J. STAT. ANN. § 56:8-1, *ET SEQ.*

(ON BEHALF OF PLAINTIFF SHETH AND THE NEW JERSEY SUB-CLASS)

104. Plaintiff Sheth incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.

105. The New Jersey Consumer Fraud Act prohibits the "use or employment by any person of any unconscionable commercial practice, deception or fraud, false pretense, false promise or misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate…is declared to be an unlawful practice…"

106. Plaintiff Sheth and the New Jersey Sub-Class never would have provided their sensitive and personal PII if they had been told or knew that Uber failed to maintain sufficient security to keep such PII from being hacked and taken by others, that Uber failed to maintain the information in encrypted form.

107. Uber's practices, acts, policies and course of conduct are actionable in that:

(a) Uber actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff Sheth and the New Jersey Sub-Class at the time they provided their PII information that Anthem did not have sufficient security or mechanisms to protect PII; and

(b) Uber failed to give adequate warnings and notices regarding the defects and problems with its defective system of security that it maintained to protect Plaintiff Sheth and the New Jersey Sub-Class' PII. Anthem possessed prior knowledge of the inherent defects in Uber's system of security and failed to give adequate and timely warnings that there had been a data breach and hacking episodes had occurred.

108. The aforementioned conduct is and was deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that Uber has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system it maintained and failed to reveal the data breach timely and adequately.

109. Members of the New Jersey Sub-Class were deceived by and relied upon Uber's affirmative misrepresentations and failures to disclose.

110. Such acts by Uber are and were deceptive acts or practices which are and/or were, likely to mislead a reasonable consumer providing their PII to Uber. Said deceptive acts and practices aforementioned are material. The requests for and use of such PII materials in New Jersey and concerning New Jersey residents and/or citizens was a consumer-oriented and thereby falls under the New Jersey Consumer Fraud Act.

111. Uber's wrongful conduct caused Plaintiff Sheth and the New Jersey Sub-Class to suffer a consumer-related injury and ascertainable losses by causing them to incur substantial expense to protect from misuse of the PII materials by third parties and placing Plaintiff Sheth and the Sub-Class at serious risk for monetary damages.

112. In addition to or in lieu of actual damages, because of the injury, Plaintiff Sheth and the New Jersey Sub-Class seek treble damages, attorneys' fees and costs for each injury and violation which has occurred.

COUNT VII

VIOLATION OF THE NEW JERSEY DATA BREACH ACT

(ON BEHALF OF PLAINTIFF SHETH AND THE NEW JERSEY SUB-CLASS)

113. Plaintiff Sheth incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.

114. Plaintiff Sheth and the other members of the New Jersey Sub-Class are riders and drivers who provided PII to Uber for personal and private use.

115. By failing to timely notify Uber customers of the Data Breach, Uber violated N.J. Stat. Ann. §56:8-163(a), et seq., which provides:

> (a) Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not

> reasonably possible. Any determination shall be documented in writing and retained for five years.
>
> * * *
>
> (c)(2) The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.
>
> * * *
>
> 56:8-166 It shall be an unlawful practice and a violation of P.L. 1960, c.39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate sections 10 through 13 of this amendatory and supplementary act.

116. The Uber Data Breach constituted a breach of the Uber security system within the meaning of the above New Jersey data breach statute and the data breached was protected and covered by the data breach statute.

117. Uber unreasonably delayed informing the public, including Plaintiff Sheth and the members of the Class, about the Data Breach after Uber knew or should have known that the Data Breach had occurred.

118. While the Data Breach and stealing of customer's personal information was known or should have been known to Uber, Uber did not notify customers of the data breach until November 21, 2017.

119. Thus, Uber failed to disclose the Data Breach to Plaintiff Sheth and the other members of the Class without unreasonable delay and in the most expedient time possible.

120. Uber has provided no indication that any law enforcement agency requested that Uber delay notification. Plaintiff Sheth and the other members of the Sub-Class suffered harm directly resulting from Uber's failure to provide and the delay in providing notification of the data breach with timely and accurate notice as required by law.

121. As a result of said practices, Uber has directly, foreseeably, and proximately caused damages to Plaintiff Sheth and the other members of the Class. Had Uber provided timely and accurate notice of the Data Breach Plaintiff Sheth and the other members of the Class would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Uber in providing notice. Plaintiff Sheth and the Class members could have avoided providing further data to Uber could have avoided use of Uber's services, and otherwise have tried to avoid the harm caused by Uber's delay in providing timely and accurate notice.

COUNT VIII

VIOLATIONS OF CALIFORNIA CONSUMER LAWS

(ON BEHALF OF PLAINTIFF LUNA AND THE CALIFORNIA SUB-CLASS)[8]

122. Plaintiff Luna incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.

[8] Upon the Cal. Civ. Code § 1782 notice requirements being satisfied, Luna and members of the proposed California Class intend to amend this count to include monetary damages in addition to the presently requested injunctive relief. Luna's counsel is notifying defendants by separate letter of the particular violations of the California Consumer Legal Remedies Act and requesting they correct or agree to correct the violations enumerated. If defendants fail to do so, Luna shall amend the complaint as of right (or otherwise seek leave to amend the complaint) to include compensatory and monetary damages.

123. Plaintiff Luna and the other members of the California Sub-Class are consumers who purchased, directly or indirectly, services from Uber for personal or family purposes.

124. Uber engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Plaintiff Luna and the other members of the California Sub-Class.

125. Uber is engaged in, and its acts and omissions affect, trade and commerce. Uber's acts, practices and omissions were done in the course of Uber's business of marketing, offering for sale, and selling goods and services in the United States, including in the state of California.

126. Uber's conduct, as alleged in this Complaint, including without limitation Uber's failure to maintain adequate computer systems and data security practices to safeguard customers' PII, Uber's failure to disclose the material fact that Uber's computer systems and data security practices, was inadequate to safeguard Insureds' PII from theft.

127. Uber's conduct constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices in violation of The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, et seq., and the California Unfair Competition Law, Cal. Bus. And Prof. Code, § 17200, et seq.

COUNT IX

VIOLATION OF THE CALIFORNIA DATA BREACH ACT (ON BEHALF OF PLAINTIFF LUNA AND THE CALIFORNIA SUB-CLASS)

128. Plaintiff Luna incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.

129. The Data Breach described above constituted a "breach of the security system" of Uber, within the meaning of Section 1798.82 (g) of the California Civil Code.

130. The information lost in the Data Breach constituted "personal information" within the meaning of Section 1798.80(e) of the California Civil Code.

131. Uber failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

132. Uber unreasonably delayed informing anyone about the breach of security of Plaintiff Luna and the California Sub-Class's confidential and non-public information after Uber knew the Data Breach had occurred.

133. Uber failed to disclose to Plaintiff Luna and the California Sub-Class, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII when they knew or reasonably believed such information had been compromised.

134. Upon information and belief, no law enforcement agency instructed Uber that notification to Plaintiff Luna and the California Sub-Class would impede investigation.

135. As a result of Defendant's violation of Cal. Civ. Code § 1798.80 et seq., Plaintiff Luna and the California Sub-Class incurred economic damages, including expenses associated with necessary credit monitoring.

136. Plaintiff Luna, individually and on behalf of the California Sub-Class, seeks all remedies available under Cal. Civ. Code § 1798.84, including but not limited to: (a) damages suffered by the California Sub-Class as alleged above; (b) statutory damages for Uber's willful, intentional, and/or reckless violation of Cal. Civ. Code § 1798.83; and (c) equitable relief.

137. Plaintiff Luna, individually and on behalf of the California Sub-Class, also seeks reasonable attorneys' fees and costs under Cal. Civ. Code § 1798.84(g).

COUNT X

VIOLATIONS OF NEW YORK'S CONSUMER PROTECTION LAWS

(ON BEHALF OF PLAINTIFF HELLER AND THE NEW YORK SUB-CLASS)

138. Plaintiff Heller incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.

139. Defendants' practices, acts, policies and course of conduct, as described above, including making representations that it possessed sufficient security to maintain the privacy of such PII, were intended to induce, and did induce, Plaintiff Heller and the New York Sub-Class to provide their sensitive PII to Uber.

140. Plaintiff Heller and the New York Sub-Class never would have provided their sensitive and personal PII if they had been told or knew that Uber failed to maintain sufficient security to keep such PII from being hacked and taken by others, that Uber failed to maintain the information in encrypted form.

141. Uber's practices, acts, policies and course of conduct are actionable in that:

(a) Uber actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff Heller and the New York Sub-Class at the time they provided such PII information that Uber did not have sufficient security or mechanisms to protect PII; and

(b) Uber failed to give adequate warnings and notices regarding the defects and problems with its defective system of security systems that it maintained to protect Plaintiff Heller and the New York Sub-Class' PII. Uber possessed prior knowledge of the inherent defects in Uber's system of security and failed to give adequate and timely warnings that there had been a Data Breach and hacking episodes had occurred.

142. The aforementioned conduct is and was deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that Uber has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system it maintained and failed to reveal the Data Breach timely and adequately.

143. Members of the public were deceived by and relied upon Uber's affirmative misrepresentations and failures to disclose.

144. Such acts by Uber are and were deceptive acts or practices which are and/or were, likely to mislead a reasonable consumer providing their PII to Uber. Said deceptive acts and practices aforementioned are material. The requests for and use of such PII materials in New York and concerning New York residents and/or citizens was a consumer-oriented act and thereby falls under the New York consumer fraud statute, General Business Law § 349 and 350.

145. Uber's wrongful conduct caused Plaintiff Heller and the New York Sub-Class to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the PII materials by third parties and placing Plaintiff Heller and the New York Sub-Class at serious risk for monetary damages.

146. In addition to or in lieu of actual damages, because of the injury, Plaintiff Heller and the Sub-Class seek statutory damages for each injury and violation which has occurred.

///

///

///

REQUEST FOR RELIEF

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

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

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

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

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

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

F. Award Plaintiffs and the other members of the Class and Sub-Classes equitable, injunctive and declaratory relief as may be appropriate under applicable laws. Plaintiffs on behalf of the other members of the Class and Sub-Classes seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing reasonable data security practices to safeguard Ubers' riders' and drivers' personal information, by an Order requiring Uber to implement reasonable data security enhancements as they become available, including data encryption, segregation of sensitive data, more robust passwords, authentication of users, increased control of access to sensitive information on the network, prohibitions of mass exports of sensitive data;

G. Enter Declaratory Judgment that seeks a declaration that (a) Uber's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Uber must implement and maintain reasonable security measures;

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

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

JURY DEMAND

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

Dated: November 24, 2017 By: *s/ Patrice L. Bishop*

Patrice L. Bishop
STULL, STULL & BRODY
9430 West Olympic Blvd., Suite 400
Beverly Hills, CA 90212
Tel: (310) 209-2468
Fax: (310) 209-2087
Email: service@ssbla.com

Howard Longman
Melissa R. Emert
STULL, STULL & BRODY
6 East 45th Street
New York, NY 10017
Tel: (212) 687-7230
Fax: (212) 490-2022
Email: hlongman@ssbny.com
memert@ssbny.com

Counsel for Plaintiffs