IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

BRADLEY WEST, individually and on behalf of all others similarly situated, Plaintiff, v. UBER USA, LLC, a limited liability company, UBER TECHNOLOGIES, INC., a California corporation, RASIER, LLC, a limited liability company, Defendants.	)	Civil Action No.: **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Bradley West ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to him and on information and belief as to all other matters, by and through undersigned counsel, hereby brings this Class Action Complaint against defendants Uber USA, LLC, Uber Technologies, Inc., and Rasier, LLC (collectively, "Uber" or "Defendant").

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against Uber for its failure to secure and safeguard the private information of approximately 57 million riders and drivers who use its service and for Uber's concealment and refusal to provide notification to individuals affected by the data breach for a period of over twelve months.

2. On November 21, 2017, Uber publicly announced a data breach that occurred back in October 2016, wherein hackers accessed Uber user data stored on a third-party cloud-based service ("Security Breach"). The Security Breach disclosed the personal information of approximately 600,000 drivers (including license information); and names, email addresses, and private cell phone numbers for approximately 57 million users. Uber allegedly paid the hackers who stole the information $100,000 in exchange for the criminals' assurance that they would delete the data. Uber failed to inform anyone of the Security Breach for more than one year from its occurrence.

3. The Security Breach was caused by Uber's knowing violation of its obligations to secure consumer information. Uber failed to comply with security standards and allowed the private information of millions collected by Uber to be compromised.

4. Accordingly, Plaintiff, on behalf of himself and all others similarly situated, asserts claims for violation of the Illinois Consumer Fraud Act, negligence, breach of contract, invasion of privacy, and unjust enrichment. Plaintiff seeks monetary damages, punitive damages, nominal damages, statutory damages, and injunctive relief, and all other relief as authorized in equity and by law.

II. JURISDICTION AND VENUE

5. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

6. The Court has personal jurisdiction over Uber because Plaintiff's claims arise out of Uber's contacts with Illinois.

7. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(2) because a substantial part of the events and omissions giving rise to the claims emanated from activities within this District.

III. PARTIES

8. Plaintiff Bradley West resides in DuPage County, Illinois, and is a citizen of the State of Illinois. Bradley West has been a user of Uber's service since January of 2016. On information and belief, Bradley West's cell phone number, name, and email address were compromised in the Security Breach. Plaintiff did not receive what he paid for.

9. Defendant Uber Technologies, Inc. is a global transportation company operating in over 600 cities worldwide. Uber Technologies, Inc. is a Delaware corporation headquartered in San Francisco, California.

10. Defendant Uber USA, LLC is an affiliate of Uber Technologies, Inc. and is a Delaware limited liability company with its principal place of business in San Francisco, California.

11. Defendant Rasier, LLC is an affiliate of Uber Technologies, Inc. and is a California limited liability company with its principal place of business in San Francisco, California.

IV. FACTUAL BACKGROUND

12. On November 21, 2017, after keeping the Security Breach secret for over a year, Uber disclosed that a breach occurred in October of 2016, during which hackers accessed Uber user data stored on a third-party cloud-based service. The Security Breach disclosed the personal

information of approximately 600,000 drivers (including license information); and names, email addresses, and private cell phone numbers for 57 million customers ("Private Information").

13. Rather than comply with its obligations to disclose such breaches and inform the public and regulators of what occurred, Uber allegedly paid the hackers behind the breach $100,000 in exchange for the criminals' silence and assurance that they would delete the data. Uber covered up the payment by calling it a bug bounty, a legitimate payment to third parties to stress test the security of their systems. Uber continued to fail to inform affected consumers of the Security Breach for more than one year.

14. The Security Breach was not the first evidence of Uber's disregard for customer privacy. On November 19, 2014, Uber founder Travis Kalanick received a letter from Senator Al Franken stating that Uber had a "troubling disregard for customer privacy" and that "it appears that on prior occasions [Uber] has condoned use of customers' data for questionable purposes."

15. On February 27, 2015, Uber announced that it suffered a data breach nine months previous, including the names and license plate numbers for approximately 50,000 drivers. Uber waited more than five months after discovering this breach to notify the people affected.

16. In August of 2017, Uber entered into a settlement with the Federal Trade Commission admitting to making false claims about the privacy of consumer data and to maintaining inadequate safeguards to protect consumer data.

17. Private Information is a valuable commodity to identity thieves. Once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years. As a result of recent large-scale data breaches, identity thieves and

cyber criminals have openly posted stolen private information directly on various Internet websites, making the information publicly available.

18. The value of Plaintiff's and Class members' Private Information on the black market is substantial. By way of the Security Breach, Uber has deprived Plaintiff and Class members of the substantial value of their Private Information and opened Uber users and their private phone numbers to nefarious elements of society and their disruptive tactics, including unwanted phone calls.

19. Uber's conduct demonstrates a willful and conscious disregard for consumer privacy. The Security Breach has exposed the private information of Plaintiff and approximately 57 million other users of Uber's service. Rather than take steps to inform the public of what occurred, Uber allegedly paid criminals in an effort to conceal the Security Breach.

V. CLASS ACTION ALLEGATIONS

20. Plaintiff brings all counts, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class defined as follows:

> All persons whose Private Information was accessed by the Security Breach. Excluded from the Class are governmental entities, Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

21. In the alternative, Plaintiff brings all counts set forth below on behalf of himself and statewide classes with laws similar to Illinois law, or further in the alternative, an Illinois class (collectively, these alternative classes are referred to as the "Illinois Class") defined as follows:

> All persons in Illinois (and in those states with laws similar to the applicable law of Illinois) whose Private Information was accessed by the Security Breach. Excluded

from the Class are governmental entities, Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

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

23. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number approximately 57 million. The precise number of Class members and their addresses are presently unknown to Plaintiff, but may be ascertained from Uber's books and records. Class members may be notified of the pendency of this action by mail, email, Internet postings, or publication.

24. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Uber failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiff's and Class members' Private Information;

b. Whether Uber properly implemented its purported security measures to protect Plaintiff's and Class members' Private Information from unauthorized capture, dissemination, and misuse;

c. Whether Uber's conduct violated data breach notification laws when it delayed notification of the Security Breach for more than a year;

d. Whether Uber intentionally concealed the existence of the Security Breach from Plaintiff and the other Class members;

e. Whether Uber took reasonable measures to determine the extent of the Security Breach after it first learned of same;

f. Whether Uber willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the other Class members' Private Information;

g. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

25. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and other Class members. Similar or identical common law and statutory violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

26. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Defendant's uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

27. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because his interests do not conflict with the interests of the other Class members he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiff and his counsel.

28. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy,

and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Uber, so it would be impracticable for Class members to individually seek redress for Uber's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS

COUNT I
Violation of Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/2
Unfair Business Practices

29. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

30. Plaintiff and the other members of the Class were subjected to Defendant's unfair or deceptive acts or practices, in violation of 815 Ill. Comp. Stat. 505/2, in failing to properly implement adequate, commercially reasonable security measures to protect their Private Information.

31. Defendant willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the Security Breach.

32. Defendant benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Security Breach.

33. Defendant willfully concealed the Security Breach and, through misrepresentations and omissions of material fact, covered up its existence by buying the hackers' assurances to keep the incident quiet.

34. Defendant's failure to implement and maintain reasonable security measures, as well as Defendant's gross misconduct in the wake of the Security Breach to conceal the Security Breach for over a year, caused and continues to cause substantial injury to Plaintiff and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

35. Defendant's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

36. Plaintiff and the other members have suffered actual damages including improper disclosure of their Private Information, lost benefit of the bargain, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

37. Plaintiff's and the other Class members' injuries were proximately caused by Defendant's violations of the ICFA, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT II
Violation of Illinois Consumer Fraud Act, 815 ILCS 505/2
Deceptive and Unfair Business Practices

38. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

39. Defendant made false representations regarding its data security practices and policies, in its privacy statement and elsewhere, including enumerating specific uses and ways in which the information could be shared.

40. These statements were false and deceptive. Defendant allowed the Security Breach to occur, which disclosed Private Information of 57 million users of Defendant's app.

41. Defendant covered up and concealed the Security Breach through knowing misrepresentations and omissions of material fact. Defendant knowingly misrepresented the ransom paid to the hackers, falsely labeling it a bug bounty. Defendant omitted the material fact that the ransom was actually paid to hackers who had executed the Security Breach.

42. These knowing misrepresentations were intended to and did conceal and delay the notification of and the investigation into the Security Breach for more than a year and failed to adequately resolve the risks and harm Plaintiff and the other Class members suffered in the Security Breach and continue to face.

43. Defendant's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

44. Plaintiff and the other Class members have suffered actual damages, including improper disclosure of their Private Information, lost benefit of the bargain, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the

Security Breach, including the increased risk of identity theft that resulted and continues to face them.

45. Plaintiff's and the other Class members' injuries were proximately caused by Defendant's violations of the ICFA, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT III
Negligence

46. Plaintiff incorporates all preceding paragraphs as if fully set forth herein.

47. Defendant owed to Plaintiff and the other Class members a duty to exercise reasonable care in handling and using personal information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from theft or unauthorized use and detect attempts at unauthorized access.

48. Defendant owed to Plaintiff and the other Class members a duty to notify them within a reasonable timeframe of any breach to the security of their personal information.

49. Defendant owed these duties to Plaintiff and the other Class members because Plaintiffs and the other Class members are a well-defined, foreseeable, and probable class of individuals whom Defendant should have been aware could be injured by Defendant's inadequate security protocols. Defendant actively solicited Plaintiff and the other Class members' personal information. Plaintiff and the other Class members were required to provide their personal information to Defendant in order to obtain services, and Defendant retained the information throughout the Plaintiffs' and other Class members' use of Defendant's services.

50. The risk that unauthorized persons would attempt to gain access to the personal information was foreseeable. As an aggregator of vast amounts of consumer data, it was inevitable

that unauthorized individuals would attempt to access Defendant's databases of personal information. Such information is valuable, and numerous instances of criminal attempts to access this kind of information have been publicized. In fact, Defendant has been targeted successfully in the past by such attempts. Defendant knew, or should have known, the risk in obtaining, using, handling, and storing the personal information of Plaintiff and the other Class members, and the importance of exercising reasonable care in handling it.

51. Defendant also owed a duty to timely and accurately disclose to Plaintiff and the other Class members the scope, nature, and occurrence of the Security Breach. This duty was required and necessary in order for Plaintiff and the other Class members to take appropriate measures to protect their information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Security Breach.

52. Defendant breached its duties by failing to exercise reasonable care in handling and securing the personal information of Plaintiff and the other Class members, which proximately caused the Security Breach and Plaintiff's and the other Class members' injuries.

53. Defendant breached its duties by failing to provide timely and accurate notice of the Security Breach to Plaintiff and the other Class members, which proximately caused and exacerbated the Security Breach, and Plaintiff's and the other Class members' injuries.

54. Defendant's failures and negligence proximately caused Plaintiff and other Class members to suffer the theft of their personal information by criminal actors and actual damages including the improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, lost time and money incurred to mitigate and remediate the

effects of the Security Breach and breach of common law duties to exercise reasonable care, including the increased risk of identity theft that resulted and continues to face them.

COUNT IV
Breach of Contract

55. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

56. Defendant entered into a contract with Plaintiff and the other Class members, which includes terms covering privacy and limiting the use and sharing of Plaintiff's and the other Class members' personal information.

57. Plaintiff and the other Class members bargained for an adequate level of security and reasonable care with respect to the use, storage, and sharing of their personal information.

58. Plaintiff and the other Class members performed their duties under the agreements.

59. Defendant violated the terms of the contract in the Security Breach by sharing Plaintiff's and the other Class members' personal information for unauthorized purposes, without first obtaining Plaintiff's or the other Class members' consent or anonymizing and/or aggregating the information in a form which cannot reasonably be used to identify them, and otherwise violating the terms of the contract.

60. Defendant violated the terms of the contract in the Security Breach by failing to take appropriate measures to protect Plaintiff's and the other Class members' personal information in accordance with its promises and representations. Defendant violated the agreement by failing to comply with applicable laws during the Security Breach regarding the access, correction, and/or deletion of personal data, and notification to affected persons.

61. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost benefit of the bargain, lost value of their

Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT V
Breach of Implied Covenant of Good Faith and Fair Dealing

62. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

63. The law implies a covenant of good faith and fair dealing in every contract.

64. Defendant entered into a contract with Plaintiff and the other Class members, which includes terms covering privacy and limiting the use and sharing of Plaintiff's and the other Class members' personal information.

65. Plaintiff and the other Class members performed their duties under the agreements.

66. Defendant's unlawful and bad faith conduct, as described above, constitutes a breach of the implied covenant of good faith and fair dealing.

67. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost benefit of the bargain, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT VI
Invasion of Privacy by Public Disclosure of Private Facts

68. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

69. Plaintiff's and the other Class members' personal information was and is private information. Plaintiff and the other Class members limit with whom the personal information is

shared, including by sharing the personal information with persons and entities whose privacy policies adequately protect the information from unknown third parties and others who might use the information for unauthorized or undesirable uses.

70. The Parties' agreement, including the Privacy Policy, contemplated that the personal information be treated as private, and be used or shared only for limited purposes.

71. Defendant disclosed Plaintiff's and the other Class members' personal information to hackers without Plaintiff's or the other Class members' authorization, consent, or knowledge.

72. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, including the increased risk of identity theft that resulted and continues to face them.

73. Defendant acted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT VII
Unjust Enrichment

74. Plaintiff pleads this count in the alternative and incorporates the factual allegations in sections I–V as if fully set forth herein.

75. Plaintiff and the other Class members conferred a monetary benefit on Defendant in the form of money paid for the purchase of services from Defendant.

76. Defendant appreciates or has knowledge of the benefits conferred directly upon them by Plaintiff and the other members of the Class.

77. Defendant knew about the Security Breach, its own deficiencies in security

practices that caused it, and its own course of conduct in covering it up through false and misleading statements and omissions.

78. It would be inequitable for Defendant to retain these benefits.

79. There is no adequately remedy at law.

80. Plaintiff and the other Class members are therefore entitled to restitution, disgorgement, and imposition of a constructive trust.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this complaint so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff Bradley West as Class Representative, and appointing Ben Barnow of Barnow and Associates, P.C. as Class Counsel;

B. Ordering Defendant to pay nominal and actual damages to Plaintiff and the other members of the Class;

C. Ordering Defendant to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

D. Ordering Defendant to pay restitution, disgorgement, and the imposition of a constructive trust on Defendant's unlawfully retained benefits;

E. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiff;

F. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded as allowable by law; and

G. Ordering such other and further relief as may be just and proper.

Date: November 28, 2017

Respectfully submitted,

Bradley West, individually and on behalf of all others similarly situated,

/s/ Ben Barnow

Ben Barnow
Erich P. Schork
Anthony L. Parkhill
Jeffrey D. Blake
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: (312) 621-2000
Fax: (312) 641-5504
b.barnow@barnowlaw.com
e.schork@barnowlaw.com
aparkhill@barnowlaw.com
j.blake@barnowlaw.com

Timothy G. Blood
Thomas J. O'Reardon
BLOOD HURST & O'REARDON, LLP
701 B Street, Suite 1700
San Diego, CA 92101
Tel: (619) 338-1100
Fax: (619) 338-1101
tblood@bholaw.com

Aron D. Robinson
THE LAW OFFICE OF ARON D. ROBSINON
180 W. Washington Street, Suite 700
Chicago, IL 60602
Tel: (312) 857-9050
Fax: (312) 857) 9054
adroblaw@aol.com