TINA WOLFSON, SBN 174806
twolfson@ahdootwolfson.com
ROBERT AHDOOT, SBN 172098
rahdoot@ahdootwolfson.com
THEODORE W. MAYA, SBN 223242
tmaya@ahdootwolfson.com
KEITH CUSTIS, SBN 218818 (Of Counsel)
keith@custis-law.com
AHDOOT & WOLFSON, P.C.
1016 Palm Ave.
West Hollywood, California 90069
Tel: 310-474-9111; Fax: 310-474-8585

Counsel for Plaintiff
SASHA ANTMAN

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

SASHA ANTMAN, individually and on behalf of all others similarly situated, Plaintiffs, v. UBER TECHNOLOGIES, INC.; and DOES 1-50, Defendant.	Case No. 15-1175 **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Sasha Antman, by and through his counsel, brings this Class Action Complaint against Defendant Uber Technologies, Inc., on behalf of himself and all others similarly situated, and alleges, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters, as follows:

PARTIES

1. Plaintiff Sasha Antman ("Plaintiff") is an individual and currently a resident of Portland, Oregon.

2. Defendant Uber Technologies, Inc. ("Defendant") is a company that conducts business throughout the United States. Defendant is a corporation organized under the laws of the state of Delaware with its principal place of business at 800 Market Street, 7th Floor, San Francisco, CA 94102.

3. Plaintiff is unaware of the true names and capacities of the defendants sued as DOES 1-50, and therefore sues these defendants by fictitious names. Plaintiff will seek leave to amend this Complaint when and if the true identities of these DOE defendants are discovered. Plaintiff is informed and believes and thereon alleges that each of the Defendants designated as a DOE is responsible in some manner for the acts and occurrences alleged herein, whether such acts or occurrences were committed intentionally, negligently, recklessly or otherwise, and that each said DOE defendant thereby proximately caused injuries and damages to Plaintiff as herein alleged, and is thus liable for the damages suffered by Plaintiff.

JURISDICTION AND VENUE

4. This Court has jurisdiction over this action under 28 U.S.C. § 1332(a) because Plaintiff and Defendant are citizens of different states.

5. The Court also has jurisdiction the Class Action Fairness Act, 28 U.S.C. § 1332 (d). The aggregated claims of the individual class members exceed $5,000,000, exclusive of interest and costs.

6. This Court has jurisdiction over Defendant because it is headquartered and

is registered to conduct business in California.

7. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant resides here, and under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL BACKGROUND

A. Defendant Failed to Notify Drivers About a Serious Data Breach It Could Have Prevented

8. Plaintiff bring this class action against Defendant for its failure to secure and safeguard its drivers' personally identifiable information including names, drivers license numbers, and other personal information ("PII") (collectively, "Private Information"), and for failing to provide timely and adequate notice to Plaintiff and other Class members that their Private Information had been stolen and precisely what types of information were stolen.

9. Defendant develops, markets, and operates a mobile-app-based transportation network called Uber. The Uber app allows consumers to submit a trip request on their smartphone, which is routed to Defendant's drivers. On information and belief, as of December 16, 2014, the service was available in 53 countries and more than 200 cities worldwide. <http://en.wikipedia.org/wiki/Uber_%28company%29> (last visited March 11, 2015).

10. Beginning in or around May 2014, an unknown person or persons (the "Hacker") utilized what Defendant has described as a "security key" to download files from Defendant's computer system containing its drivers' Private Information (the "Data Breach"). (Complaint in *Uber Techs., Inc. v. Doe*, N.D. Cal. Case No. 15-cv-00908-LB, Docket No. 1, filed 2/27/15.)

11. Defendant did not disclose the Data Breach until February 27, 2015, when it disseminated a press release stating, *inter alia*, "In late 2014, we identified a one-time access of an Uber database by an unauthorized third party. . . ." <http://blog.uber.com/2-27-15> (last visited March 11, 2015) (the "Press Release").

12. Defendant admits in its Press Release that it knew of the Data Breach at least as early as September 17, 2014 — over ***five months*** before Defendant issued the Press Release or made any effort whatsoever to notify Plaintiff and other Class Members that their Private Information had been disclosed in the Data Breach. (*Id.*)

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

14. Defendant also stated in its Press Release that it "filed what is referred to as a 'John Doe' lawsuit so that we are able to gather information that may lead to confirmation of the identity of the third party." (*Id.*) On information and belief, this refers to the *Doe* complaint cited *supra*.

15. News reports and a subpoena issued by Defendant in connection with the above-described *Doe* proceedings indicate that the "security key" used by the Hacker to perpetrate the Data Breach was publicly available on the internet via one or more GitHub webpages (and/or via the GitHub app, which is an app designed for sharing code among app developers). *See, e.g.*, <http://www.theregister.co.uk/2015/02/28/uber_subpoenas_github_for_hacker_details> (last visited March 11, 2015). In other words, Defendant not only permitted all of the compromised Private Information to be accessible via a single password, but allowed that password to be publicly accessible via the internet.

16. On information and belief, Defendant could have prevented this Data Breach. It appears that Defendant maintained the Private Information in unencrypted form, and that the Hacker was able to access it freely with a basic password.

17. Defendant thus disregarded Plaintiff's and Class members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose to thos

affected the facts that it did not have adequate computer systems and security practices in place, or that the Data Breach had occurred in a timely manner. On information and belief, Plaintiff's and Class members' Private Information and the password allowing access to that Private Information were improperly handled and stored, were unencrypted, and were not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiff's and Class members' Private Information was compromised and stolen.

B. Plaintiff Was Damaged By the Data Breach

18. Plaintiff previously worked as an Uber driver in San Francisco, receiving his last payment for such services in or around September 2013.

19. On or around June 2, 2014, an unknown and unauthorized person used Plaintiff's Private Information to apply for a credit card with Capital One, which now appears on Plaintiff's credit report.

20. Plaintiff received notification from Defendant in or around March 2015, notifying him for the first time that his Private Information was disclosed in the Data Breach, even though he no longer was working as an Uber driver at the time of the Data Breach.

21. Defendant's notification to Plaintiff did not include any explanation for the long delay in its issuance or indicate that the delay was due to any law enforcement investigation.

C. The Stolen Private Information Is Valuable to Hackers and Thieves and Its Disclosure Harms Class Members

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

23. Legitimate organizations and the criminal underground alike recognize the value in PII. Otherwise, they wouldn't pay for it or aggressively seek 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 from 38 million users."[1]

24. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." *Id*.

25. Unfortunately, Defendant's apparent approach at maintaining the privacy of Plaintiffs' and Class members' PII, which relied solely on a password, was lackadaisical, cavalier, reckless, or at the very least, negligent.

26. The ramifications of Defendant's failure to keep Class members' data secure are severe.

27. The information compromised, including Class members' identifying information, is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC").[2] Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year.

28. 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."[3]

29. Identity thieves can use personal information such as that of Class members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government

---

[1] Verizon 2014 PCI Compliance Report, available at <http://www.nocash.info.ro/wp-content/uploads/2014/02/ Verizon_pci-report-2014.pdf> (hereafter "2014 Verizon Report"), at 54 (last visited Sept. 12, 2014).

[2] FTC Interactive Toolkit, Fighting Back Against Identity Theft, *available at* <http://www.dcsheriff.net/community/documents/id-theft-tool-kit.pdf> (last visited March 11, 2015).

[3] FTC, Signs of Identity Theft, available at <http://www.consumer.ftc.gov/articles/0271-signs-identity-theft> (last visited March 11, 2015).

fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years.

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

31. 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 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.[4]

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

[4] GAO, Report to Congressional Requesters, at p.33 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf> (emphases added) (last visited March 11, 2015).

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

a. theft of their Private Information;

b. misuse of their Private Information such as the unauthorized attempt to open a credit card account in Plaintiff's name described above, and additional such injury threatened in the future;

c. damage to Plaintiff's and Class members' credit reports and/or scores;

d. the untimely and inadequate notification of the Data Breach;

e. loss of privacy;

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

g. deprivation of rights they possess under California law, including the Consumer Records Act and Business and Professions Code § 17200, *et seq*.

34. Defendant's offer of one-year of free identity protection services, including credit monitoring, is insufficient compensation for damages resulting from Defendant's actions and inactions because (a) that offer was made months after Defendant learned of the breach, during which time Plaintiff's and other Class members' Private Information was misused; (b) such credit monitoring does not prevent or retroactively fix the damage done to Class members and their credit reports; and (c) as the GAO reported, the PII could be held by criminals and used to commit fraud after the one year of credit monitoring and identity theft protection expires.

CLASS ACTION ALLEGATIONS

35. Plaintiff seeks relief in his individual capacity and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2) and/or (b)(3), Plaintiff seeks certification of a national class and a California class. The national class initially is defined as follows:

> All persons residing in the United States whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2014 (the "National Class").

36. The California Class is initially defined as follows:

> All persons residing in California whose personal information was disclosed in the data breach affecting Uber Technologies, Inc. in 2014 (the "California Class).

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

38. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, based on Defendant's statements Private Information pertaining to at least "50,000 drivers across multiple states" was disclosed in the Data Breach.

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

a. Whether Defendant violated California Civil Code § 1798.81.5 by failing to implement reasonable security procedures and practices;

b. Whether Defendant violated California Civil Code § 1798.82 by failing to promptly notify class members their personal information had been compromised;

c. Whether class members may obtain an injunctive relief against Defendant under Civil Code § 1798.84 or under the UCL;

d. What security procedures and data-breach notification procedure should Defendant be required to implement as part of any injunctive relief ordered by the Court;

e. Whether Defendant has an express or implied contractual obligation to use reasonable security measures;

f. Whether Defendant has complied with any express or implied contractual obligation to use reasonable security measures;

g. Whether Defendant violated California Business and Professions Code § 17200, *et seq.*; and

h. The nature of the relief, including equitable relief, to which Plaintiff and the Class members are entitled.

40. Ascertainability. All members of the purposed Classes are readily ascertainable. Defendant has access to addresses and other contact information for all, or substantially all, members of the Classes, which can be used for providing notice to many Class members.

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

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

43. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this

controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

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

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

COUNT I

For Violation of the Civil Code Sections 1798.81.5 & 1798.82

(On Behalf of Plaintiff and the California Class)

46. Plaintiff incorporates the substantive allegations above as if fully set forth herein.

47. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code section 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

48. The Private Information taken in the Data Breach fits within the definition of "Personal information" in Civil Code section 1798.80.

49. Plaintiff and other Class members provided their personal information to Defendant in order to use the Uber App to generate income by providing services as Uber drivers, and thus qualify as "Customer[s]" as defined in Civil Code section

1798.80.

50. Defendant failed to dispose of Plaintiff's Private Information after he no longer was working as an Uber driver, thus allowing that Private Information to be compromised in the Data Breach that occurred when he no longer was working as an Uber driver and violating Civil Code section 1798.81.

51. By failing to implement reasonable measures to protect its drivers' Private Information, Defendant violated Civil Code section 1798.81.5.

52. In addition, by failing to promptly notify all affected drivers that their Private Information had been acquired (or was reasonably believed to have been acquired) by the Hacker(s) in the Data Breach, Defendant violated Civil Code Section 1798.82.

53. As a direct or proximate result of Defendant's violations of Civil Code Sections 1798.81, 1798.81.5, and 1798.82, Plaintiff and Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in this Class Action Complaint, including in Paragraphs 31-33, *supra*.

54. Defendant's violations of Civil Code Sections 1798.81, 1798.81.5, and 1798.82 were, at a minimum, reckless, including by virtue of the fact that the Private information apparently was not encrypted and the password allowing access to it was made available on a publicly accessible website.

55. In addition, by violating Civil Code Sections 1798.81, 1798.81.5, and 1798.82, Defendant "may be enjoined" under Civil Code Section 1798.84(e).

56. Defendant's violations of Civil Code Section 1798.81.5 and 1798.82 also constitute an unlawful acts or practices under California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 et seq., which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

57. Plaintiff accordingly requests that the Court enter an injunction requiring Defendant to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendant utilize strong industry standard encryption

algorithms for encryption keys that provide access to stored PII; (2) ordering that Defendant implement the use of its encryption keys in accordance with industry standards; (3) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis; (4) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendant audit, test and train its security personnel regarding any new or modified procedures; (6) ordering that Defendant, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's computer system is compromised, hackers cannot gain access to other portions of its systems; (7) ordering that Defendant purge, delete, destroy in a reasonable secure manner customer data not necessary for its ongoing relationship with drivers; (8); ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendant, consistent with industry standard practices, evaluate web applications for vulnerabilities to prevent web application threats to drivers; (10) ordering that Defendant, consistent with industry standard practices, periodically 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 (11) ordering Defendant to meaningfully educate its drivers and former drivers about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

58. Plaintiff further requests that the Court require Defendant to identify and notify all members of the Class who have not yet been informed of the Data Breach, and to notify affected drivers and/or users of its app of any future data breaches by email within 24 hours of Defendant's discovery of a breach or possible breach and by

mail within 72 hours.

59. Plaintiff and the Class are entitled to actual damages in an amount to be determined at trial under Civil Code Section 1798.84.

60. Plaintiff and the Class also are entitled to an aware of attorney fees and costs under Civil Code Section 1798.84.

COUNT II

Violation of California Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq*.

(On Behalf of Plaintiffs and the California Class)

61. Plaintiff incorporates the substantive allegations above as if fully set forth herein.

62. Defendant engaged in unfair, fraudulent and unlawful business practices in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. ("UCL").

63. Plaintiff suffered injury in fact and lost money or property as a result of Defendant's alleged violations of the UCL.

64. The acts, omissions, and conduct of Defendant as alleged constitutes a "business practice" within the meaning of the UCL.

65. Defendant violated the unlawful prong of the UCL by violating Civil Code Sections 1798.81.5 and 1798.82, as alleged above.

66. Defendant's acts, omissions, and conduct also violate the unfair prong of the UCL because those acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiff and other Class members. The harm cause by Defendant's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendant's legitimate business interests, other than Defendant's conduct described herein.

67. Defendant's conduct also undermines California public policy — as reflected in statutes like the Information Practices Act, Cal. Civ. Code § 1798 *et seq.*,

and the California Customer Records Act, Cal. Civ. Code §§ 1798.81.5 and 1798.82 concerning customer records — which seek to protect customer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

68. By failing to disclose that it does not enlist industry standard security practices, which render Defendant's app and services particularly vulnerable to data breaches, Defendant engaged in a fraudulent business practice that is likely to deceive a reasonable consumer.

69. A reasonable person would not have agreed to use the Uber app or to act as an Uber driver had he or she known the truth about Defendant's security procedures. By withholding material information about Defendant's security practices, it was able to convince drivers and other users of its app to provide and entrust their Private Information to Defendant.

70. Defendant's failure to disclose that it does not enlist industry standard security practices also constitutes an unfair business practice under the UCL. Defendant's conduct is unethical, unscrupulous, and substantially injurious to Class members.

71. As a result of Defendant's violations of the UCL, Plaintiff and the other Class members are entitled to injunctive relief including, but not limited to: (1) ordering that Defendant utilize strong industry standard encryption algorithms for encryption keys that provide access to stored PII; (2) ordering that Defendant implement the use of its encryption keys in accordance with industry standards; (3) ordering that Defendant, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis; (4) ordering that Defendant engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendant audit, test and train its security

personnel regarding any new or modified procedures; (6) ordering that Defendant, consistent with industry standard practices, segment PII by, among other things, creating firewalls and access controls so that if one area of Defendant's computer system is compromised, hackers cannot gain access to other portions of its systems; (7) ordering that Defendant purge, delete, destroy in a reasonably secure manner PII not necessary for its provisions of services; (8); ordering that Defendant, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that Defendant, consistent with industry standard practices, evaluate smartphone and web applications for vulnerabilities to prevent threats to drivers and other users of the Uber app; (10) ordering that Defendant, consistent with industry standard practices, periodically 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 (11) ordering Defendant to meaningfully educate its drivers and riders about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps such drivers and riders must take to protect themselves.

72. As a result of Defendant's violations of the UCL, Plaintiff and other Class members have suffered injury in fact and lost money or property, as detailed in Paragraphs 30 through 32 of this Class Action Complaint. Plaintiff requests that the Court issue sufficient equitable relief to restore Class members to the position they would have been in had Defendant not engaged in unfair competition, including by ordering restitution of all funds that Defendant acquired as a result of its unfair competition, including fees that Defendant retained for rides given by Plaintiff and other Class members.

///

///

REQUEST FOR RELIEF

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

A. For an Order certifying this action as a class action and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to its data collection, storage, and safety practices and to disclose with specificity to Class members the type of data compromised in the Data Breach, and other information required under Cal. Civ. Code § 1798.82;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;

F. For an award of costs of suit and attorneys' fees, as allowable by law; and

G. Such other and further relief as this court may deem just and proper.

///

///

///

///

DEMAND FOR JURY TRIAL

Plaintiff demands trial by jury of all claims so triable.

Dated: March 12, 2015

Respectfully submitted,

AHDOOT & WOLFSON, PC

Tina Wolfson
Robert Ahdoot
Theodore W. Maya
Bradley King
Keith Custis (Of Counsel)
AHDOOT & WOLFSON, PC
1016 Palm Ave.
West Hollywood, California 90069
Telephone: 310-474-9111
Facsimile: 310-474-8585

Counsel for Plaintiff
SASHA ANTMAN