Byron T. Ball (SBN 150195)
THE BALL LAW FIRM
644 S. Figueroa Street
Los Angeles, California 90017
Attorneys for Plaintiffs J. DOE 1; J. DOE 2;
J. DOE 3; J. DOE 4; and J. DOE 5

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

J. DOE 1; J. DOE 2; J. DOE 3; J. DOE 4; and J. DOE 5, individually and on behalf of all others similarly situated,	§	
Plaintiffs,	§	
v.	§	**CASE NO. _____**
AVID LIFE MEDIA, INC. a Canadian corporation; and AVID DATING LIFE, INC. d/b/a Ashley Madison	§	
Defendants.	§	

CLASS ACTION COMPLAINT

Plaintiffs J. Doe 1, J. Doe 2, J. Doe 3, J. Doe 4, and J. Doe 5 individually and on behalf of the Classes defined below of similarly situated persons, (hereafter, collectively, "Plaintiffs"), allege the following against Defendant Avid Life Media, Inc." ("Avid Life") and Defendant Avid Dating Life, Inc. d/b/a Ashley Madison ("Ashley Madison"), (hereafter, collectively, "Defendants"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

SUMMARY OF ACTION

1. This action seeks redress for Defendants' failure to secure and safeguard its users' personal information.

2. Defendants operate a website, AshleyMadison.com, that is marketed with the slogan, "Life is Short. Have an Affair."

3. From their website, Defendants obtain private personal information, ("PPI"), such as name, address, e-mail address, height, weight, sexual fantasies, and sexual preferences from their customers and maintain the PPI on their servers. Defendants also obtain and store their customers' personal financial information, ("PFI"), such as credit card numbers and passwords, on its servers

4. Defendants have touted Ashley Madison as being secure on numerous occasions. *See* http://fusion.net/story/185052/7-times-ashley-madisons-ceo-bragged-about-the-sites-amazing-privacy-features/.

5. In reliance on Defendants' representations regarding the security of the data collected, Plaintiffs and members of the Class subscribed to Defendants' services and provided the information that Defendants requested/required.

6. On or about July 19, 2015, hackers, calling themselves "The Impact Team" claimed that they had obtained PPI and PFI on millions of individuals, who subscribed or had subscribed to Ashley Madison. http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/. The hackers threatened to release the PPI and PFI of Defendants' customers' if its website wasn't shut down.

7. Defendants did not shut down their site or secure their customers' information and, on August 20, 2015, the hackers released the PPI and PFI of millions of current and former subscribers to AshleyMadison.com, (the "Security Breach").

8. Defendants' security failures enabled intruders to access and seize customers' PPI and PFI.

9. Published reports indicate that the PPI and PFI of millions of Defendants' current and former customers from around the United States was compromised in the Security Breach. *See* *http://abcnews.go.com/Technology/wireStory/qa-ashley-madison-hack-latest-high-profile-breach-33212867*.

10. The PPI the hackers released was of a highly sensitive and personal nature, whose disclosure, not to mention the very fact that a person had an account with Ashley Madison, is likely to and has caused Plaintiffs' extreme emotional distress/embarrassment, disruption of/interference with Plaintiffs' personal and social life, and/or economic loss.

11. The PFI the hackers released subjects Plaintiffs to a heightened risk of fraud, fraudulent charges, and/or identity theft.

12. Plaintiffs' PPI and PFI is at serious and ongoing risk of misuse – the hackers and/or others may to use the data they obtained as a result of Defendants' inadequate security to exploit Plaintiffs.

13. Plaintiffs retain a significant interest in ensuring that their PPI and PFI is protected from further breaches, and seek to remedy the harms they have suffered as a result of the Security Breach.

14. Plaintiffs assert claims against Defendants for violations of state data breach statutes, breach of state consumer protection laws, breach of implied contract, negligence, public disclosure of private fact, and breach of contract. Plaintiffs seek to recover damages, including actual and statutory damages, and equitable relief, including injunctive relief to prevent a recurrence of the Security Breach and resulting injury, restitution, disgorgement and reasonable costs and attorneys' fees.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

16. This Court has personal jurisdiction over Defendants because they market their products in and regularly conduct business in California. Defendants intentionally avail themselves of this jurisdiction by marketing and selling products in California and by conducting business in California with certain of the Plaintiffs and members of the Class. Defendants have sufficient minimum contacts with California to render the exercise of jurisdiction by this Court permissible.

17. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(a) and (b) because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District. Further, Defendants actively solicit California residents to use its services.

PARTIES

18. Plaintiffs reallege, as if fully set forth, each and every allegation herein.

19. Plaintiff J. Doe 1 is citizen of the State of California who resides in this District.

20. Plaintiff J. Doe 2 is a citizen of the State of Georgia.

21. Plaintiff J. Doe 3 is a citizen of the State of Tennessee.

22. Plaintiff J. Doe 4 is a citizen of the State of Texas.

23. Plaintiff J. Doe 5 is a citizen of the State of Minnesota.

24. At this time, Plaintiffs bring this litigation under a pseudonym to prevent public disclosure of their identity and to protect information highly sensitive and personal to them and to prevent further invasion of their privacy. Plaintiffs will disclose their identity to Defendants'

counsel and/or this Court upon demand and pursuant to a protective order to be entered by the Court.

25. Defendant Avid Life is a Canadian corporation with headquarters in Toronto, Ontario, Canada.

26. Defendant Avid Dating Life, Inc. d/b/a Ashley Madison is a Canadian corporation with headquarters in Toronto, Ontario, Canada.

27. Plaintiffs and the Class members have suffered actual injury from having his or her PPI and/or PFI accessed and seized in and as a result of the Security Breach.

28. Plaintiffs and the Class members have suffered actual injury in the form of emotional distress and/or economic loss.

29. Plaintiffs and the Class members have suffered imminent and impending injury arising from the release of their PPI and/or a substantially increased risk of future fraud, identity theft and misuse posed by his or her PFI being released to the public as a result of the Security Breach. Plaintiffs have a continuing interest in ensuring that their PPI and PFI, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

STATEMENT OF FACTS

30. Defendants operate AshleyMadison.com to help individuals find other individuals looking for sexual encounters. Defendants market AshleyMadison.com with the slogan, "Life is short. Have an Affair" and target married individuals for their matchmaking services. As part of their business, Defendants store vast amounts of personal information of individuals throughout the United States.

31. The personal information stored by Defendants includes, but is not necessarily limited to: name, username, hashed password, security question and answer, email address, date

of birth, height, weight, and photos. Defendants also obtained and stored PPI such as the person's sexual fantasies and the types of sexual encounters in which the person was willing to engage. Defendants also obtained and stored PFI such as the person's billing address, credit card number, credit card expiration date, and security code.

32. On information and belief, an untold number of individuals became the victims of the Security Breach when personal information, of the type described in paragraph 31, was accessed and seized from Defendants' information systems.

33. On July 19, 2015 hackers, calling themselves "The Impact Team," claimed to have obtained personal information of millions of individuals who subscribed or had subscribed to Ashley Madison. *See* http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/. The hackers threatened to release the personal information of Defendants' customers' if AshleyMadison.com was not shut down.

34. Defendants did not shut down AshleyMadison.com or secure their customers' personal information and, August 20, 2015, the hackers released the PPI and PFI of millions of current and former subscribers to AshleyMadison.com, (the "Security Breach"). The information was originally posted on the "Dark Web" but it was quickly picked up and shared by dozens of other more easily accessible websites, some going so far as to make the data searchable. *See* http://www.wired.com/2015/08/check-loved-one-exposed-ashley-madison-hack/.

35. The consequences of this information becoming public have been described as "catastrophic," subjecting those who used AshleyMadison.com to severe consequences such as interference with job loss and prosecution – not to mention the effect that this information may

have on the individual's marriage and other personal relationships. *See eg.* http://www.theverge.com/2015/8/19/9178855/ashley-madison-data-breach-implications.

36. Although Defendants' CEO Noel Biderman routinely bragged about his company's security. Defendants did not, in fact, implement reasonable security standards. Indeed, internal documents show that Defendants were well-aware of the potential for hackers to take their customers' personal information well before the hack actually occurred. *See http://www.csoonline.com/article/2973575/business-continuity/ashley-madison-self-assessments-highlight-security-fears-and-failures.html*

37. Further, even once Defendants knew that their customers personal information had been hacked, they failed to take reasonable steps to prevent the data's public disclosure or prevent further data from being stolen.

38. Moreover, Defendants provided false and/or misleading information about the nature and extent of the information stolen, initially denying that the data came from their site; it has since been confirmed that the data did, in fact, come from Defendants. *See* https://krebsonsecurity.com/2015/08/was-the-ashley-madison-database-leaked/.

Security Breaches Lead to Identity Theft

39. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying data to open financial accounts, receive government benefits and incur charges and credit in a person's name.[1] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's

[1] *See* http://www.gao.gov/new.items/d07737.pdf (last visited August 3, 2015).

credit rating. In addition, the GAO Report states that victims of identity theft "face substantial costs and time to repair the damage to their good name and credit record."[2]

40. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumer's finances, credit history and reputation and can take time, money and patience to resolve.[3] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[4]

41. A person who's PFI has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [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.

Personal Information is Valuable Property

42. At a FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's PFI as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve]

---

[2] *Id*. at 2.

[3] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited August 3, 2015).

[4] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC 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," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

> Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[5]

43. Though Commissioner Swindle's remarks are more than a decade old, they are even more relevant today, as Personal Information functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[6]

44. The FTC has also recognized that PFI is a new – and valuable – form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[7]

45. Recognizing the high value that consumers place on their personal information, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information that they share – and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from the surrender of their personal

---

[5] *The Information Marketplace: Merging and Exchanging Consumer Data*, https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited August 3, 2015).

[6] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited August 3, 2015).

[7] *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited August 3, 2015).

information.[8] This business has created a new market for the sale and purchase of this valuable data.[9]

46. Defendants recognize the value of their customers' personal information by offering to erase this data for the payment of a $19 fee. However, even when customers paid the fee, Defendants did not actually erase all of the customers' data. As a result, even Plaintiffs who paid the $19 fee had PPI and/or PFI stolen in the Security Breach and publicly released.

47. Consumers place a high value not only on their personal information, but also on the *privacy* of that data. Researchers have already begun to shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[10]

48. Defendants recognized the importance of its customers' privacy and touted the security of its systems in the marketing of its products. *See e.g.* http://fusion.net/story/185052/7-times-ashley-madisons-ceo-bragged-about-the-sites-amazing-privacy-features/.

[8] *You Want My Personal Data? Reward Me for It*, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited August 3, 2015).

[9] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited August 3, 2015).

[10] Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (June 2011), pre-publication version available at http://www.heinz.cmu.edu/~acquisti/papers/acquisti-onlinepurchasing-privacy.pdf (last visited August 5, 2015).

49. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their PFI – the very injury at issue here – between $11.33 and $16.58 per website.[11]

50. The value of customers' PPI is less easily measured but significantly more valuable. Indeed, but for Defendants' representations that their PPI would be kept private, Plaintiffs and the Class members would not have used AshleyMadison.com.

51. Given these facts, any company that transacts business with a consumer and then compromises the privacy of its customers' personal information has deprived that customer of the full monetary value of the transaction.

52. In further recognition of the value of its customers' personal information, Defendants offered to completely delete or erase customer's Personal Information from its systems/records in exchange for payment of a $19 fee.

53. Plaintiff J. Doe 4 and other members of the Class paid the $19 fee. Defendant, however, did not delete or erase Plaintiff J. Doe 4's or other members of the Class' Personal Information. Accordingly, Plaintiff J. Doe's and other members of the Class' Personal Information was still on Defendants' systems/records and was subject to and was, in fact, stolen by hackers in the Security Breach.

Damages Sustained By Plaintiffs and the Class

54. A portion of the services Plaintiffs and the Class purchased from Defendants necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of personal information. Indeed, due to representations made by Defendants

[11] Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.200.6483&rep=rep1&type=pdf (emphasis added) (last visited August 3, 2015).

regarding the security of the data they maintain, Plaintiffs and the Class members reasonably expected that Defendants would provide a *higher* level of security than other service companies.

55. Because Plaintiffs and the Class members were denied privacy protections that they were entitled to and reasonably expected to receive, Plaintiffs and the Class have been damaged.

56. Plaintiffs and the Class members have suffered extreme emotional distress/embarrassment, disruption of/interference with Plaintiffs' personal and social life, and/or economic loss as a result of Defendants' failure to properly secure the PPI.

57. Plaintiffs and the Class members suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Defendants' failure to secure their PFI.

58. Moreover, as explained above, fraudulent use of PI might not be apparent for years. Therefore, customers must expend considerable time taking these precautions for years to come.

59. Plaintiffs and the Class suffered additional damages based on the opportunity cost and value of time that Plaintiffs and the Class have been forced to expend to monitor their PFI as a result of the Security Breach.

60. Plaintiffs and the Class have suffered damages as a result of Defendants' failure to delete or erase their Personal Information from its systems/records as agreed.

CLASS ALLEGATIONS

61. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert their claims that Defendants violated state data breach notification statutes (Count I) on behalf of separate statewide classes defined as follows:

> **Statewide Data Breach Notification Classes:**
> All residents of [name of State] whose Personal Information was compromised as a result of the Ashley Madison data breach first disclosed in July of 2015.

62. Plaintiffs assert the state data breach notification law claims (Count I) on behalf of separate statewide classes in and under the respective data breach statutes of the States of Alaska, California, Colorado, Delaware, Georgia, Hawaii, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Michigan, Montana, New Hampshire, New Jersey, North Carolina, North Dakota, Oregon, South Carolina, Tennessee, Virginia, Washington, Wisconsin and Wyoming, and the District of Columbia.

63. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert their claims that Defendants violated state consumer protection law (Count II) on behalf of separate statewide classes defined as follows:

> **Statewide Consumer Protection Classes:**
> All residents of [name of State] whose Personal Information was compromised as a result of the Ashley Madison data breach first disclosed in July of 2015.

64. Plaintiffs assert the state consumer law claims (Count I) under the listed consumer protection laws of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South

Dakota, Tennessee, Texas, Utah, Vermont, Virginia, U.S. Virgin Islands, Washington, West Virginia, Wyoming, and the District of Columbia.

65. Pursuant to Fed. R. Civ. P.23, Plaintiff J. Doe 1 ("California Plaintiff") asserts a claim under the California Customer Records Act, California Civil Code section 1798.81.5, and the "unlawful prong" of California's Unfair Competition Law, California Business and Professions Code section 17200 (Count III) on behalf of a California class defined as follows:

> **California Class:**
> All residents of California whose Personal Information was compromised as a result of the Ashley Madison data breach first disclosed in July 2015.

66. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert their common law claims for breach of implied contract (Count IV), negligence (Count V), and public disclosure of private fact (Count VI), on behalf of a nationwide class, defined as follows:

> **Nationwide Class:**
> All residents of the United States whose Personal Information was compromised as a result of the Ashley Madison data breach first disclosed in July of 2015.

67. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims for breach of implied contract (Count IV), negligence (Count V), and public disclosure of private fact (Count VI), under the laws of the individual States and Territories of the United States, and on behalf of separate statewide classes, defined as follows:

> **Statewide [Breach of Implied Contract, Negligence & Privacy] Classes:**
> All residents of [name of State] whose Personal Information was compromised as a result of the Ashley Madison data breach first disclosed in July 2015.

68. Pursuant to Fed. R. Civ. P. 23, Plaintiffs assert their common law claims for breach of contract (Count VII) on behalf of a nationwide class, defined as follows:

Nationwide Class:
All residents of the United States who paid Defendants a fee to have their Personal Information deleted/erased and whose Personal Information was compromised as a result of the Ashley Madison data breach first disclosed in July of 2015.

69. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims for breach of contract (Count VII) under the laws of the individual States and Territories of the United States, and on behalf of separate statewide classes, defined as follows:

Statewide [Breach of Contract] Classes:
All residents of [name of State] who paid Defendants a fee to have their Personal Information deleted or erased and whose Personal Information was compromised as a result of the Ashley Madison data breach first disclosed in July 2015.

70. Excluded from each of the above Classes are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

71. Excluded from each of the above Classes are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

72. Each of the proposed classes meet the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3):

73. **Numerosity.** The proposed classes include millions of individuals whose PPI and/or PFI was compromised in the Security Breach. While the precise number of Class

members in each proposed class has not yet been determined, the massive size of the Security Breach indicates that joinder of each member would be impracticable.

74. **Commonality.** Common questions of law and fact exist and predominate over any questions affecting only individual Class members. The common questions include:

a. whether Defendants engaged in the conduct alleged herein;

b. whether Defendants had a legal duty to provide timely and accurate notice of the Security Breach to Plaintiffs;

c. whether Defendants breached their duty to provide timely and accurate notice of the Security Breach to Plaintiffs;

d. whether and when Defendants knew or should have known that their computer systems were vulnerable to attack;

e. whether Defendants misrepresented the security of their systems;

f. whether Defendants had a legal duty to adequately protect Plaintiffs' PPI and PFI;

g. whether Defendants breached their legal duty by failing to adequately protect Plaintiffs' PPI and PFI;

h. whether Defendants' conduct in allowing Plaintiffs' PPI and/or PFI to be publicly revealed is extreme and outrageous;

i. whether Defendants caused private facts about Plaintiffs to be publicly revealed;

j. whether Plaintiffs are entitled to recover actual damages and/or statutory damages; and

k. whether Plaintiffs are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

75. **Typicality.** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and Class members were injured as a result of Defendants' uniform misconduct and their legal claims arise from the same core practices/failures.

76. **Adequacy.** Plaintiffs are adequate representatives of the proposed classes because their interests do not conflict with the interests of the Class members they seek to represent. Plaintiffs' counsel is very experienced in litigating consumer class actions, data breach class actions and complex commercial disputes.

77. **Superiority.** A class action is superior to all other available methods of fairly and efficiently adjudicating this dispute. The injury sustained by each Class member, while meaningful on an individual basis, is not of such magnitude that it is economically feasible to prosecute individual actions against Defendants. Even if it were economically feasible, requiring hundreds of thousands of injured plaintiffs to file individual suits would impose a crushing burden on the court system and almost certainly lead to inconsistent judgments. By contrast, class treatment will present far fewer management difficulties and provide the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

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

79. Finally, all members of the purposed Classes are readily ascertainable. Defendants have access to addresses and other contact information for members of the Classes, which can be used to identify Class members.

COUNT I

VIOLATIONS OF STATE DATA BREACH NOTIFICATION STATUTES

(ON BEHALF OF PLAINTIFFS AND THE SEPARATE STATEWIDE DATA BREACH STATUTE CLASSES)

80. Plaintiffs reallege, as if fully set forth, each and every allegation herein.

81. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally apply to any person or business conducting business within the state that owns or licenses computerized data containing personal information. If the personal information is acquired or accessed in a way that compromises its security or confidentiality, the covered entity must notify the affected individuals in the most expedient time and manner possible and without unreasonable delay.

82. The Security Breach constituted a breach that triggered the notice provisions of the data breach statutes and the information taken includes categories of personal information protected by the data breach statutes.

83. Defendants unreasonably delayed in informing Plaintiffs and members of the statewide Data Breach Statute Classes ("Class," as used in this Count I), about the data breach after Defendants knew or should have known that the data breach had occurred.

84. Plaintiffs and Class members were damaged by Defendants' failure to comply with the data breach statutes.

85. Had Defendants provided timely and accurate notice, Plaintiffs and Class members could have avoided or mitigated the harm caused by the Security Breach.

86. Defendants' failure to provide timely and accurate notice of the Security Breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), et seq.;

b. Cal. Civ. Code § 1798.80, et seq.;

c. Colo. Rev. Stat. Ann § 6-1-716(2), et seq.;

d. Del. Code Ann. Tit. 6 § 12B-102(a), et seq.;

e. D.C. Code § 28-3852(a), et seq.;

f. Ga. Code Ann. § 10-1-912(a), et seq.;

g. Haw. Rev. Stat. § 487N-2(a), et seq.;

h. Ill. Comp. Stat. Ann. 530/10(a), et seq.;

i. Iowa Code Ann. § 715C.2(1), et seq.;

j. Kan. Stat. Ann. § 50-7a02(a), et seq.;

k. Ky. Rev. Stat. Ann. § 365.732(2), et seq.;

l. La. Rev. Stat. Ann. § 51:3074(A), et seq.;

m. Md. Code Ann., Commercial Law § 14-3504(b), et seq.;

n. Mich. Comp. Laws Ann. § 445.72(1), et seq.;

o. Mont. Code Ann. § 30-14-1704(1), et seq.;

p. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), et seq.;

q. N.J. Stat. Ann. § 56:8-163(a), et seq.;

r. N.C. Gen. Stat. Ann. § 75-65(a), et seq.;

s. N.D. Cent. Code Ann. § 51-30-02, et seq.;

t. Or. Rev. Stat. Ann. § 646A.604(1), et seq.;

u. S.C. Code Ann. § 39-1-90(A), et seq.;

v. Tenn. Code Ann. § 47-18-2107(b), et seq.;

w. Va. Code Ann. § 18.2-186.6(B), et seq.;

x. Wash. Rev. Code Ann. § 19.255.010(1), et seq.;

y. Wis. Stat. Ann. § 134.98(2), et seq.; and

z. Wyo. Stat. Ann. § 40-12-502(a), et seq.

87. Plaintiffs and members of each of the statewide Data Breach Statute Classes seek all remedies available under their respective state data breach statutes, including but not limited to damages, equitable relief, including injunctive relief, treble damages, reasonable attorneys' fees and costs, as provided by the applicable laws.

COUNT II

VIOLATIONS OF STATE CONSUMER PROTECTION LAWS

(ON BEHALF OF PLAINTIFFS AND THE SEPARATE STATEWIDE CONSUMER PROTECTION CLASSES)

88. Plaintiffs reallege, as if fully set forth, each and every allegation herein.

89. Plaintiffs and members of the statewide Consumer Law Classes (the "Class" for purposes of this claim) are consumers who paid for services from Defendants through AshleyMadison.com.

90. Defendants 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 Plaintiffs and members of the Class.

91. Defendants are engaged in, and their acts and omissions affect, trade and commerce. Defendants' acts, practices, and omissions were done in the course of business of marketing, offering for sale, and selling goods and services throughout the United States.

92. Defendants' conduct constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices (collectively, "Deceptive Trade Practices"), including, among other things, Defendants':

a. Failure to maintain adequate computer systems and data security practices to safeguard customers' Personal Information;

b. Failure to disclose that its computer systems and data security practices were inadequate to safeguard customers' Personal Information from theft;

c. Representing that its computer systems and data security practices were sufficient to maintain the security of Plaintiffs' and the Class members' personal information when, in fact, they were not;

d. Representing that if customers paid a fee their personal information would be deleted or erased when, in fact, it was not;

e. Failure to timely and accurately disclose the data breach to Plaintiffs and Class members;

f. Continued acceptance of Plaintiffs' and Class members' credit and debit card payments and storage of other personal information after Defendants knew or should have known of the security vulnerabilities that were exploited in the data breach; and

g. Continued acceptance of Plaintiffs' and Class members' credit and debit card payments and storage of other personal information after Defendants knew or should have known of the data breach and before it allegedly fixed the breach.

93. By engaging in such Deceptive Trade Practices, Defendants have violated state consumer laws, including those that prohibit:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

b. Representing that goods and services are of a particular standard, quality or grade, if they are of another;

c. Omitting material facts regarding the goods and services sold;

d. Engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding;

e. Unfair methods of competition; unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices; and/or similar prohibitions under the state consumer laws identified below.

94. As a direct result of Ashley Madison's violating state consumer laws, Plaintiffs and Class members suffered damages that include:

a. Purchasing products and services from Ashley Madison that they would not have purchased, or would have not had paid the same price for, had they known of Defendants' Deceptive Trade Practices;

b. Fraudulent charges on their debit and credit card accounts, some of which have not been reimbursed;

c. Theft of their Personal Information by criminals;

d. Costs associated with the detection and prevention of identity theft;

e. Costs associated with the fraudulent use of their financial accounts;

f. Loss of use of and access to some or all of their account funds and costs incurred as a result of being unable to access those funds;

g. Costs and lost time associated with handling the administrative consequences of the Security Breach, including identifying, disputing, and seeking

reimbursement for fraudulent charges, canceling and activating payment cards, and shopping for credit monitoring and identity theft protection;

h. Impairment to their credit scores and ability to borrow and/or obtain credit; and

i. The continued risk to their personal information, which remains on Defendants' insufficiently secured computer systems.

95. Ashley Madison's Deceptive Trade Practices violate the following state consumer statutes:

a. The Alabama Deceptive Trade Practices Act, Ala. Code §§ 8-19-5(2), (3), (5), (7), and (27), et seq.;

b. The Alaska Unfair Trade Practices and Consumer Protection Act, Alaska Stat. §§ 45.50.471-45.50.561;

c. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

d. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107(a)(1)(10) and 4-88-108(1)(2), et seq.;

e. 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.;

f. The Colorado Consumer Protection Act, Col. Rev. Stat. Ann. §§ 6-1-105(1)(b), (c), (e) and (g), et seq.;

g. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), et seq.;

h. The Delaware Consumer Fraud Act, Del. Code Ann. Title 6 § 2513, et seq.;

i. The District of Columbia Consumer Protection Act, D.C. Code §§ 28-3904(a), (d), (e), (f) and (r), et seq.;

j. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), et seq.;

k. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-393(a) and (b)(2), (3), (5), and (7), et seq.;

l. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), et seq., and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), et seq.;

m. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), et seq., and Idaho Code § 48-603C, et seq.;

n. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, et seq., and the Illinois Uniform Deceptive Trades Practices Act, 815 Ill. Stat. §§ 510/2(a)(5), (7) and (12), et seq.;

o. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-3(a) and (b)(1) and (2), et seq.;

p. The Kansas Consumer Protection Act, Kan. Stat. §§ 50-626(a) and (b)(1)(A)(D) and (b)(3), et seq.;

q. The Kentucky Consumer Protection Act, Ky. Rev. Stat. §§ 367.170(1) and (2), et seq.;

r. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), et seq.;

s. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), et seq.;

t. The Maine Uniform Deceptive Trade Practices Act, 10 M.R.S.A. §§ 1212(1)(E) and (G), et seq., and the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207, et seq.;

u. The Maryland Consumer Protection Act, Md. Code Commercial Law, §§ 13-301(1) and (2)(i)-(ii), and (iv), (5)(i), and (9)(i), et seq.;

v. The Michigan Consumer Protection Act, M.C.P.L.A. §§ 445.903(1)(c)(e), (s) and (cc), et seq.;

w. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), et seq., and the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(a);

x. The Mississippi Consumer Protect Act, Miss. Code Ann. §§ 75-24-5(1), (2)(b), (c), (e), and (g), et seq.;

y. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), et seq.;

z. The Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. § 30-14-103, et seq.;

aa. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 591602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), et seq.;

bb. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. §§ 598.0915(5) and (7), et seq.;

cc. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2(v) and (vii), et seq.;

dd. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, et seq.; The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7) and (14) and 57-12-3, et seq.;

ee. The New York Business Law, N.Y. Gen. Bus. Law § 349(a);

ff. The North Carolina Unfair Trade Practices Act, N.C.G.S.A. § 75-1.1(a), et seq.;

gg. The North Dakota Unlawful Sales or Advertising Practices Act, N.D. Cent. Code § 51-15-02, et seq.;

hh. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. §§ 1345.02(A) and (B)(1) and (2), et seq.;

ii. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. §§ 753(5), (7) and (20), et seq.;

jj. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. §§ 646.608(1)(e)(g) and (u), et seq.;

kk. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, et seq.;

ll. The Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws §§ 6-13.1-1(6)(v), (vii), (xii), (xiii) and (xiv), et seq.;

mm. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), et seq.;

nn. The South Dakota Deceptive Trade Practices Act and Consumer Protection Act, S.D. Codified Laws § 37-24-6(1), et seq.;

oo. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-104(a), (b)(2), (3), (5), and (7), et seq.;

pp. The Texas Deceptive Trade Practices Consumer Protection Act, V.T.C.A., Bus. & C. §§ 17.46(a), (b)(5) and (7), et seq.;

qq. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-4(1), (2)(a), (b), and (i) et seq.;

rr. The Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a), et seq.;

ss. The Virgin Islands Consumer Protection Law, V.I. Code Ann. tit. 12A, § 101, et seq.;

tt. The Virginia Consumer Protection Act, Va. Code Ann. §§ 59.1-200(A)(5)(6) and (14), et seq.;

uu. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, et seq.;

vv. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, et seq.; and

ww. The Wyoming Consumer Protection Act, Wyo. Stat. Ann. §§ 40-12-105(a), (i), (iii) and (xv), et seq.

96. As a result of Defendants' violations, Plaintiffs and members of the Class are entitled to injunctive relief, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including

simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

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

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

d. Ordering that Defendants segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems are compromised, hackers cannot gain access to other portions of their systems;

e. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services without additional charge to the customer;

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

g. Ordering that Ashley Madison 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 Defendants 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 the customers must take to protect themselves.

97. Because of Defendants' Deceptive Trade Practices, Plaintiffs and the Class members are entitled to relief, including restitution of the costs associated with the data breach, disgorgement of all profits accruing to Defendants because of its Deceptive Trade Practices, attorneys' fees and costs, declaratory relief, and a permanent injunction Defendants from their Deceptive Trade Practices.

98. Plaintiffs bring this claim on behalf of themselves and the Class members for the relief requested and to benefit the public interest. This claim supports the public interests in assuring that consumers are provided truthful, non-deceptive information about potential purchases and protecting members of the public from Defendants' Deceptive Trade Practices. Defendants' wrongful conduct, including its Deceptive Trade Practices has affected the public at large because a substantial percentage of the U.S. population has been affected by their conduct.

COUNT III

VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT, CALIFORNIA CIVIL CODE § 1798.81.5 AND THE CALIFORNIA UNFAIR COMPETITION LAW'S UNLAWFUL PRONG

(ON BEHALF OF CALIFORNIA PLAINTIFF AND THE CALIFORNIA CLASS)

99. Plaintiffs reallege, as if fully set forth, each and every allegation herein.

100. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted the Customer Records Act, California Civil Code §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."

101. As described above, Defendants failed to implement and maintain reasonable security procedures and practices to protect the California Plaintiff's and California Class members' PPI and PFI, and thereby violated California Civil Code section 1798.81.5.

102. By violating section 1798.81.5 of the California Customer Records Act, Defendants are liable to the California Plaintiff and California Class members for damages under California Civil Code section 1798.84(b).

103. Because Defendants "violates, proposes to violate, or has violated," the California Customer Records Act, the California Plaintiff is entitled to injunctive relief under California Civil Code section 1798.84(e).

104. In addition, Defendants' violations of the Customer Records Act constitute unlawful acts or practices under California's Unfair Competition Law, California Business and Professions Code sections 17200, et seq., which provides for restitution damages, and grants the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

105. Accordingly, the California Plaintiff requests that the court enter an injunction that requires Defendants to implement reasonable security procedures and practices, including, but not limited to: (1) ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors; (2) ordering that Defendants engage third-party security auditors and internal personnel

to run automated security monitoring; (3) ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Defendants segment data by, among other things, creating firewalls and access controls so that if one area of Defendants are compromised, intruders cannot gain access to other portions of Defendants' systems; (5) ordering that Defendants purge, delete, and destroy in a reasonably secure manner data not necessary for its provisions of services; (6) ordering that Defendants conduct regular database scanning and securing checks; (7) ordering that Defendants 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 (8) ordering Defendants to meaningfully educate its users about the threats they face as a result of the loss of their PPI and PFI to third parties, as well as the steps Defendants users must take to protect themselves.

106. The California Plaintiff and members of the California Class seek all remedies available under the California Customer Records Act and the California Unfair Competition Law, including but not limited to, restitution, damages, equitable relief, including injunctive relief, reasonable attorneys' fees and costs, and all other relief allowed under the applicable laws.

COUNT IV

BREACH OF IMPLIED CONTRACT

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE BREACH OF IMPLIED CONTRACT CLASSES)

107. Plaintiffs reallege, as if fully set forth, each and every allegation herein.

108. When Plaintiffs and the members of the Nationwide class or, alternatively, the members of the separate Statewide Breach of Implied Contract Classes (collectively, the "Class"

as used in this Count), provided their PPI and PFI to Defendants, they entered into implied contracts by which Defendants agreed to protect their PPI and PFI and timely notify them in the event of a data breach.

109. An implicit part of the agreement regarding Defendants' use of PPI and PFI was that Defendants would safeguard the PPI and PFI using reasonable or industry-standard means and would timely notify Plaintiffs in the event of a data breach.

110. Based on the implicit understanding, Plaintiffs and the Class provided Defendants with their PPI and PFI.

111. Plaintiffs and Class members would not have provided their PPI and PFI to Defendants had they known that Defendants would not safeguard their PPI and PFI as promised or provide timely notice of a data breach.

112. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendants.

113. Defendants breached the implied contracts by failing to safeguard Plaintiffs' and Class members' PPI and PFI and failing to provide them with timely and accurate notice when their PPI and PFI was compromised in the Security Breach.

114. The losses and damages Plaintiffs and Class members sustained (as described above) were the direct and proximate result of Defendants' breaches of its implied contracts with them.

COUNT V

NEGLIGENCE

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

115. Plaintiffs reallege, as if fully set forth, each and every allegation herein.

116. Defendants owed numerous duties to Plaintiffs and to members of the Nationwide Class, or, alternatively, members of the separate Statewide Negligence Classes (collectively, the "Class" as used in this Count). Defendants' duties included the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PPI and PFI in their possession;

b. to protect their PPI and PFI using reasonable and adequate security procedures and systems that are consistent with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Class members of the Security Breach.

117. Defendants owed a duty of care not to subject Plaintiffs and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices. Defendants solicited, gathered, and stored Plaintiffs' and Class members' PPI and PFI as part of their general course of business.

118. Defendants knew, or should have known, of the risks inherent in collecting and storing PPI and PFI and the importance of adequate security. Defendants also knew about

numerous, well-publicized data breaches. Defendants touted the security of their data as a reason for customers to use its services.

119. Defendants knew, or should have known, that their computer systems did not adequately safeguard Plaintiffs' and Class members' PPI and PFI.

120. Because Defendants knew that a breach of their systems would damage millions of individuals, including Plaintiffs and Class members, they had a duty to adequately protect their PPI and PFI.

121. Defendants had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' willingness to entrust Defendants with their PPI and PFI was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their computer systems and the PPI and PFI it stored on them from attack.

122. Defendants also had independent duties under state laws that required Defendants to reasonably safeguard Plaintiffs' and Class members' PPI and PFI and promptly notify them about the Security Breach.

123. Defendants breached the duties it owed to Plaintiffs and Class members in numerous ways, including:

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

b. by failing to implement adequate security systems, protocols and practices sufficient to protect their PPI and PFI both before and after learning of the Security Breach;

c. by failing to comply with the minimum industry data security standards during the period of the Security Breach; and

d. by failing to timely and accurately disclose that their PPI and/or PFI had been improperly acquired or accessed.

124. But for Defendants' wrongful and negligent breach of the duties it owed Plaintiffs and Class members, their PPI and PFI either would not have been compromised or they would have been able to prevent some or all of their damages.

125. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Defendants' negligent conduct. Accordingly, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT VI

PUBLIC DISCLOSURE OF PRIVATE FACT

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

126. Plaintiffs reallege, as if fully set forth, each and every allegation herein.

127. Defendants published private facts about Plaintiffs' and Class members.

128. The private facts that Defendants published are so intimate and their publication so unwarranted that the community's notions of decency are outraged.

129. The private facts about Plaintiffs' and Class members are not of legitimate public concern.

130. Plaintiffs and Class members have suffered harm as a direct and proximate result of Defendants' publication of the private facts.

COUNT VII

BREACH OF CONTRACT

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

131. Plaintiffs reallege, as if fully set forth, each and every allegation herein.

132. In exchange for payment of a fee, Defendants agreed to delete or erase a customers' Personal Information from its systems/records.

133. Plaintiff J. Doe 4 and other members of the Class paid the fee to have their Personal Information deleted or erased from Defendants' systems/records.

134. Defendants did not delete or erase Plaintiff J. Doe 4's and other Class members' Personal Information from its systems/records.

135. Defendants breached the contract with Plaintiff J. Doe 4 and other Class members by not deleting or erasing their Personal Information as agreed.

136. Plaintiff J. Doe 4 and other members of the Class had their Personal Information stolen in the Security Breach.

137. Plaintiff J. Doe 4 and other members of the Class have been damages as a direct and proximate result of Defendants' breach of the contract.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes set forth herein, respectfully request that the Court enter judgment in their favor that:

A. certifies the Classes requested, appoints Plaintiffs as class representatives of the applicable classes and their undersigned counsel as Class counsel;

B. awards the Plaintiffs and Class members appropriate monetary relief, including actual and statutory damages, restitution, and disgorgement,

C. on behalf of Plaintiffs and the Statewide Classes, enters an injunction that requires Defendants to implement and maintain adequate security measures, including the measures specified above to ensure the protection of Plaintiffs' PPI and PFI, which remains in the possession of Defendants;

D. on behalf of Plaintiffs and the Statewide Data Breach Statute Classes, awards appropriate equitable relief, including an injunction requiring Defendants to promptly notify all affected customers of future data breaches;

E. orders Defendants to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

F. awards Plaintiffs and the Classes pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

G. awards such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

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

August 24, 2015

Respectfully submitted,

s/Byron T. Ball

Byron T. Ball
THE BALL LAW FIRM
644 S. Figueroa Street
Los Angeles, California 90017
Telephone: (310) 446-6148
btb@balllawllp.com

William B. Federman*
Carin L. Marcussen*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
405.235.1560 (*telephone*)
405.239.2112 (*facsimile*)
wbf@federmanlaw.com
clm@federmanlaw.com
www.federmanlaw.com

* Admission *pro hac vice* to be sought

Counsel to Plaintiffs