IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

JANE DOE (a pseudonym) On behalf of herself and all others similarly situated	)	
Plaintiffs,	)	**Case Number:**
vs.	)	**JURY TRIAL DEMANDED**
AVID LIFE MEDIA, INC. a corporation,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

NOW COMES the Plaintiff Jane Doe (a pseudonym), on behalf of herself and all others similarly situated, and for her class action complaint states as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action as a result of a breach of the security system of Defendant AVID LIFE MEDIA INC. (ALM) governing electronic transactions, resulting in compromised security of Plaintiff's and Class Members' personal financial information. Upon information and belief such personal information included, but upon information and belief was not limited to, the putative Class Members' (hereafter "Class Members") names, addresses, credit or debit card number, the card's expiration date, and/or the card's CVV (a three-digit security code) ("Personal Information").

2. On or about July 15 of this year, and at times prior, ALM's databases were compromised, with the result that Personal Information of Plaintiff and Class Members' Personal Information was used or is at risk of use in fraudulent transactions around the world, as well as other invidious exposure. Upon information and belief, Defendant maintains or maintained

information, including Personal Information, regarding nearly 37 million subscribers, and Defendant's security failures affected the credit and debit card of hundreds of thousands if not millions of customers, including Plaintiff and Class Members.

3. Upon information and belief, the security breach and theft of Personal Information was caused by Defendant's violations of its obligations to abide by the best practices and industry standards concerning the security of its payment processing systems and the computers associated therewith as set forth, for example, in Payment Card Industry Security Standards Council Data Security Standards ("PCI DSS") and the decisions of the Federal Trade Commission ("FTC") concerning protection of consumer financial information.

4. After learning of the security breach, Defendant failed to notify Plaintiff and the putative Classes in a timely manner and failed to take other reasonable steps to inform them of the nature and extent of the breach. As a result, Defendant prevented Plaintiffs and the putative Class Members from protecting themselves from the breach and caused Plaintiffs and Class Members to suffer financial loss.

5. Plaintiff, on behalf of herself and all others similarly situated, asserts the following claims: Violations of the Stored Communications Act ("SCA"), 18 U.S.C. § 2702; negligence; breach of implied contract; violations of the Missouri Merchandising Practices Act ("MMPA"), Mo. Rev. Stat. § 407.020, and the substantially similar statutes of the other states in which Defendant conducts business.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, which confers upon the Court original jurisdiction over all civil actions arising under the laws of the

United States, and pursuant to 18 U.S.C. § 2707. This Court has supplemental jurisdiction over Plaintiff's and Class Members' state law claims under 28 U.S.C. § 1367.

7. In addition, this Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all Members of the putative Classes are in excess of $5,000,000.00, exclusive of interest and costs, and many of the Members of the putative Classes are citizens of different states than Defendant. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d).

8. Venue is properly set in this District pursuant to 28 U.S.C. § 1391(b) since Defendant transacts business within this judicial district. Likewise, a substantial part of the events giving rise to the claim occurred within this judicial district.

PARTIES

9. Plaintiff Jane Doe (a pseudonym) is an adult female domiciled in Maryland Heights, Missouri and is a citizen of Missouri. Jane Doe provided her Personal Information to Defendant in order to effectuate a "paid-delete" of any of her personal information in Defendant's possession, including her Personal Information, as promised by Defendant. On information and belief Doe's Personal Information was compromised as a result of Defendant's security failures. As a result of such compromise, Doe suffered losses and damages in an amount yet to be completely determinable as such losses and damages are ongoing.

10. On information and belief Defendant is a corporation organized under Canadian law with its headquarters and principal place of business in Toronto, Canada.

FACTUAL BACKGROUND

11. Defendant is a merchant that owns, operates, and controls social networking services, including a site on the Internet branded as "Ashley Madison".

12. Upon information and belief, Defendant's data breach has impacted hundreds of thousands, or millions of its customers nationwide within the United States.

13. Hackers accessed a database owned, operated, or controlled by ALM that processes, stores, or utilizes information regarding ALM transactions, with account numbers, expiration dates, card holder names and/or other information, on information and belief.

14. Plaintiff Jane Doe herein contacted Defendant to accept Defendant's offer to "paid-delete" any personal information, including Personal Information, in Defendant's possession; in other words, Defendant promised to delete such information for a fee ($19, on information and belief).

15. Defendant broke such promise to Plaintiff and the Class Members, who also sought a "paid-delete."

16. Upon information and belief, the Defendant accepts customer payments for services through credit and debit cards issued by members of the payment card industry ("PCI") such as Visa or MasterCard.

17. In 2006, the PCI members established a Security Standards Counsel ("PCI SSC") as a forum to develop PCI Data Security Standards ("PCI DSS") for increased security of payment processing systems.

18. The PCI DSS provides, "If you are a merchant that accepts payment cards, you are required to be compliant with the PCI Data Security Standard." Defendant, or course, is a merchant that accepts payment cards.

19. The PCI DSS requires a merchant to:

a. **Assess**—identify cardholder data, take inventory of IT assets and business processes for payment card processing, and analyze them for vulnerabilities that could expose cardholder data.

b. **Remediate**—fix vulnerabilities and do not store cardholder data unless needed.

c. **Report**—compile and submit required remediation validation records (if applicable) and submit compliance reports to the acquiring bank and card brands with which a merchant does business.

20. Additionally, since 1995, the FTC has been studying the manner in which online entities collect and use personal information and safeguards to assure that online data collection practice is fair and provides adequate information privacy protection. The result of this study is the FTC Fair Information Practice Principles. The core principles are:

a. **Notice/Awareness--**Consumers should be given notice of an entity's information practices before any personal information is collected from them. This requires that companies explicitly notify of some or all of the following:

- Identification of the entity collecting the data;
- Identification of the uses to which the data will be put;
- Identification of any potential recipients of the data;
- The nature of the data collected and the means by which it is collected;
- Whether the provision of the requested data is voluntary or required; and
- The steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

b. **Choice/Consent--**Choice and consent in an online information-gathering sense means giving consumers options to control how their data is used with respect to secondary uses of information beyond the immediate needs of the information collector to complete the consumer's transaction.

c. **Access/Participation--**Access as defined in the Fair Information Practice Principles includes not only a consumer's ability to view the data collected, but also to verify and contest its accuracy. This access must be inexpensive and timely in order to be useful to the consumer.

d. **Integrity/Security--**Information collectors should ensure that the data they collect is accurate and secure. They should improve the integrity of data by cross-referencing it with only reputable databases and by providing access for the consumer to verify it. Information collectors should keep their data secure by protecting against both internal and external security threats. They should limit access within their company to only necessary employees to protect against internal threats, and they should use encryption and other computer-based security systems to stop outside threats.

e. **Enforcement/Redress--**In order to ensure that companies follow the Fair Information Practice Principles, there must be enforcement measures. The FTC identifies three types of enforcement measures: self-regulation by the information collectors or an appointed regulatory body; private remedies that give civil causes of action for individuals whose information has been misused to sue violators; and government enforcement, which can include civil and criminal penalties levied by the government.

21. On information and belief, Defendant failed to adequately analyze its computer systems for vulnerabilities that could expose cardholder data. Defendant further failed to fix the

vulnerabilities in its computer systems which allowed Plaintiff's and Class Members' Personal Information to become compromised.

22. Additionally, on information and belief, Defendant unlawfully collected consumer financial data for marketing purposes beyond the needs of specific transactions, in order to accrue financial benefit at the risk and likelihood of compromising consumers' Personal Information.

23. As a result, Defendant allowed Personal Information connected with thousands of consumers' credit cards and debit cards, including credit cards and debit cards of Plaintiff and Class Members, to become compromised for a period prior to July 15 of this year.

24. Plaintiff and Class Members are subject to continuing damage from having their Personal Information comprised as a result of Defendant's inadequate systems and failures. Such damages include, among other things, the amount paid to Defendant to perform a "paid-delete" which Defendant did not perform or performed inadequately; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendant's security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards; and irrecoverable financial losses due to unauthorized charges on the credit/debit cards of Defendant's customers by identity thieves who wrongfully gained access to the Personal Information of Plaintiffs and the Classes.

CLASS ACTION ALLEGATIONS

25. Plaintiff brings this action on her own behalf and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following three (3) multi-state classes:

> All persons in the United States who paid Defendant for "paid-delete" services which were improperly performed.
>
> All persons in the United States whose Personal Information was subject to Defendant's security failures and who suffered damages in the amount of fraudulent charges / unauthorized withdrawals made to their credit and/or debit cards or suffered damages in the amount of overdraft charges made to their credit and/or debit cards.
>
> All persons in the United States whose Personal Information was subject to Defendant's security failures and who have suffered or anticipate suffering damages, loss, and/or expenses accruing due to Defendant's security failures.

Excluded from the Classes are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors.

26. The Members of the Classes are so numerous that joinder of all Members is impracticable. On information and belief, thousands, hundreds of thousands, or more credit and/or debit cards may have been compromised, and the Members of the Classes are geographically dispersed. Disposition of the claims of the proposed Classes in a class action will provide substantial benefits to both the parties and the Court.

27. The rights of each member of the proposed Classes were violated in a similar fashion based upon Defendant's uniform wrongful actions and/or inaction.

28. The following questions of law and fact are common to each proposed Class Member and predominate over questions that may affect individual Class Members:

a. Whether Defendant failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' private financial information;

b. Whether Defendant properly implemented its purported security measures to protect consumers' private financial information from unauthorized capture, dissemination and misuse;

c. Whether Defendant took reasonable measures to determine the extent of the security breach after it first learned of the same;

d. Whether Defendant's delay in informing consumers of the security breach was unreasonable;

e. Whether Defendant's method of informing consumers of the security breach and its description of the breach and potential exposure to damages as a result of the same was unreasonable;

f. Whether Defendant's conduct violated the Stored Communications Act, 18 U.S.C. § 2702;

g. Whether Defendant breached an implied contract with Class Members;

h. Whether Defendant's conduct violated the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.020, and the substantively similar statutes of the other states where Defendant conducts business; and

i. Whether Plaintiffs and others Members of the Classes are entitled to compensation, monetary damages, equitable relief and injunctive relief, and, if so, the nature and amount of such relief.

29. Plaintiff's claims are typical of the claim of absent Class Members. If brought individually, the claim of each Class Member would necessarily require proof of the same material and substantive facts, and seek the same remedies.

30. The Plaintiffs are willing and prepared to serve the Court and the proposed Classes in a representative capacity. The Plaintiffs will fairly and adequately protect the interest of the Classes and have no interests adverse to, or which directly and irrevocably conflicts with, the interests of other Members of the Classes. Further, Plaintiffs have retained counsel experienced in prosecuting complex class action litigation.

31. Defendant has acted or refused to act on grounds generally applicable to the proposed Classes, thereby making appropriate equitable relief with respect to the Classes.

32. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual claims by the Class Members are impractical, as the costs of prosecution may exceed what any Class Member has at stake.

33. Members of the Classes are readily ascertainable through Defendant's records of the transactions it undertook.

34. Prosecuting separate actions by individual Class Members would create a risk of inconsistent or varying adjudications that would establish incomparable standards of conduct for Defendant. Moreover, adjudications with respect to individual Class Members would, as a practical matter, be dispositive of the interests of other Class Members.

CAUSES OF ACTION

COUNT I – VIOLATION OF THE FEDERAL STORED COMMUNICATIONS ACT, 18 U.S.C. § 2702

35. Plaintiffs repeat, reallege, and incorporate paragraphs 1-40 in this Complaint as if fully set forth herein.

36. The Stored Communications Act ("SCA") contains provisions that provide consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, "to protect individuals' privacy interests in personal and

proprietary information." S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 at 3557.

37. Section 2702(a)(1) of the SCA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

38. The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." Id. at § 2510(15).

39. Through its payment processing equipment, Defendant provides an "electronic communication service to the public" within the meaning of the SCA because it provides consumers at large with credit and debit card payment processing capability that enables them to send or receive wire or electronic communications concerning their private financial information to transaction managers, card companies, or banks.

40. By failing to take commercially reasonable steps to safeguard sensitive private financial information, even after Defendant was aware that customers' Personal Information had been compromised, Defendant has knowingly divulged customers' private financial information that was communicated to financial institutions solely for customers' payment verification purposes, while in electronic storage in Defendant's payment system.

41. Section 2702(a)(2)(A) of the SCA provides that "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing

of communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

42. The SCA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communication system." 18 U.S.C. § 2711(2).

43. An "electronic communications systems" is defined by the SCA as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(4).

44. Defendant provides remote computing services to the public by virtue of its computer processing services for consumer credit and debit card payments, which are used by customers and carried out by means of an electronic communications system, namely the use of wire, electromagnetic, photooptical or photoelectric facilities for the transmission of wire or electronic communications received from, and on behalf of, the customer concerning customer private financial information.

45. By failing to take commercially reasonable steps to safeguard sensitive private financial information, Defendant has knowingly divulged customers' private financial information that was carried and maintained on Defendant's remote computing service solely for the customer's payment verification purposes.

46. As a result of Defendant's conduct described herein and its violations of Section 2702(a)(1) and (2)(A), Plaintiff and putative Class Members have suffered injuries, including lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft. Plaintiff, on her own behalf and on behalf of the putative Classes, seek

an order awarding themselves and the Classes the maximum statutory damages available under 18 U.S.C. § 2707 in addition to the cost for 3 years of credit monitoring services.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count I of their Complaint; for actual and compensatory damages; for punitive or exemplary damages; for punitive or exemplary damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT II – NEGLIGENCE

47. Plaintiffs repeat, reallege, and incorporate the preceding paragraphs of this Complaint as if fully set forth herein.

48. Upon coming into possession of Plaintiff's and Class Members' Personal Information, i.e., private, non-public, sensitive financial information, Defendant had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the information from being compromised and/or stolen.

49. Defendant also had a duty to timely disclose to Plaintiff and Class Members that a breach of security had occurred and their Personal Information pertaining to their credit cards and/or debit cards had been compromised, or was reasonably believed to be compromised.

50. Defendant also had a duty to put into place internal policies and procedures designed to detect and prevent the theft or dissemination of Plaintiff's and Class Members' Personal Information.

51. Defendant, by and through its above negligent acts and/or omissions, breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and

safeguarding their Personal Information which was in Defendant's possession, custody, and control.

52. Defendant, by and through its above negligent acts and or omissions, further breached its duty to Plaintiffs and Class Members by failing to put into place internal policies and procedures designed to detect and prevent the unauthorized dissemination of Plaintiff and Class Members' Personal Information.

53. Defendant, by and through its above negligent acts and or omissions, breached its duty to timely disclose the fact that Plaintiff and Class Members' Personal Information had been or was reasonable believed to be have been compromised.

54. Defendant's negligent and wrongful breach of its duties owed to Plaintiff and Class Members, their Personal Information would not have been compromised.

55. Plaintiff's and Class Members' Personal Information was compromised and/or stolen as a direct and proximate result of Defendant's breach of its duties as set forth herein.

56. Plaintiff and Class Members have suffered actual damages including, but not limited to, having their personal information compromised, incurring time and expenses in cancelling their debit and/credit cards, activating new cards and re-establishing automatic payment authorizations from their new cards, and other economic and non-economic damages, including irrecoverable losses due to unauthorized charges on their credit/debit cards.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count II of their Complaint; for actual and compensatory damages; for punitive or exemplary damages; for punitive or exemplary damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT III -- BREACH OF IMPLIED CONTRACT

57. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

58. Plaintiffs and Class Members were required to provide Defendant with their Personal Information in order to facilitate their credit card and/or debit card transactions.

59. Implicit in this requirement was a covenant requiring Defendant to take reasonable efforts to safeguard this information and promptly notify Plaintiffs and Class Members in the event their information was compromised.

60. Similarly, it was implicit that Defendant would not disclose Plaintiff's and Class Members' Personal Information.

61. Notwithstanding its obligations, Defendant knowingly failed to safeguard and protect Plaintiff's and Class Members' Personal Information. To the contrary, Defendant allowed this information to be disseminated to unauthorized third parties.

62. Defendant's above wrongful actions and/or inaction breached its implied contracts with Plaintiffs and Class Members, which in turn directly and/or proximately caused Plaintiffs and Class Members to suffer substantial injuries.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count III of their Complaint; for actual and compensatory damages; for punitive or exemplary damages; for punitive or exemplary damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT IV – VIOLATION OF THE MISSOURI MERCHANDISING PRACTICES ACT AND SUBSTANTIALLY SIMILAR STATUTES OF THE OTHER STATES WHERE DEFENDANT DOES BUSINESS

63. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

64. Defendant violated the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.020, and the substantially similar statutes of the other states in which it conducts business by failing to properly implement adequate, commercially reasonable security measures to protect customers' private financial information, and by failing to immediately notify affected customers of the nature and extent of the security breach.

65. Defendant's fraudulent and deceptive omissions and misrepresentations regarding the company's security measures to protect customers' private financial information and the extent of the breach of those security measures were intended to deceive and induce Plaintiffs and the putative Class Members' reliance on Defendant's misrepresentations that their financial information was secure and protected when using debit and credit cards to shop at Defendant stores.

66. Defendant's unlawful misrepresentations and omissions occurred in the course of conduct involving trade or commerce.

67. Defendant's unlawful misrepresentations and omissions were material because Plaintiffs and the other putative Class Members, if they had known the truth, would not have risked compromising their private financial information by using their debit or credit cards at Defendant stores. Plaintiffs and the other putative Class Members would consider the omitted and misrepresented material facts important in making their purchasing decisions.

68. Defendant's unlawful misrepresentations and omissions damaged Plaintiffs and the other putative Class Members because Plaintiffs and Class Members would not have chosen to expose their private financial information to a security breach and subsequent exploitation by the defrauders.

69. Plaintiffs, individually and on behalf of the putative Classes, seek an order requiring Defendant to pay: monetary and punitive damages for the conduct described herein; three years of credit card fraud monitoring services for Plaintiffs and Members of the putative Classes; and the reasonable attorney's fees and costs of suit of Plaintiffs and Class Members; together with all such other and further relief as may be just.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count IV of their Complaint; for actual and compensatory damages; for punitive or exemplary damages; for punitive or exemplary damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

COUNT V – BREACH OF CONTRACT

70. Plaintiffs repeat, reallege, and incorporate the foregoing paragraphs of this Complaint as if fully set forth herein.

71. Defendant promised Plaintiff and the Class Members, for a fee of approximately $19, to delete any of Plaintiff's/Class Member's personal information, including Personal Information, in Defendant's possession (the "paid-delete" service).

72. On information and belief, Defendant broke such promise, and did not delete some or all of Plaintiff's/Class Member's Personal Information in Defendant's possession, even after the payment of such fee.

73. Plaintiffs have been damage thereby in the amount paid to the Defendant to perform a "paid-delete," and in the amount of other losses as previously stated.

WHEREFORE Plaintiff and Class Members pray for Judgment in their favor and against Defendant on this Count V of their Complaint; for actual and compensatory damages; for punitive or exemplary damages; for punitive or exemplary damages; for punitive or exemplary damages; for injunctive relief; for costs, expenses and attorney fees as allowed by law; and for such other and further relief as this Court deems just and proper.

JURY TRIAL DEMAND

Plaintiffs and class members demand a jury trial as to all claims and issues triable of right by a jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Members of the proposed Classes pray that this Honorable Court do the following:

A. Certify the matter as a class action pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and order that notice be provided to all Class Members;

B. Designate Plaintiffs as representative of the Classes and the undersigned counsel as Class Counsel;

C. Award Plaintiffs and the Classes compensatory and punitive damages in an amount to be determined by the trier of fact;

D. Award Plaintiffs and the Classes statutory interest and penalties;

E. Award Plaintiffs and the Classes appropriate injunctive and/or declaratory relief;

F. Award Plaintiffs and the Classes their costs, prejudgment interest, and attorney fees; and

G. Grant such other relief as is just and proper.

Respectfully submitted,
THE DRISCOLL FIRM, P.C.

By: /s/John J. Driscoll

John J. Driscoll, #6276464
211 N. Broadway, 40th Floor
St. Louis, Missouri 63102
314-932-3232 telephone
314-932-3233 facsimile