Joshua B. Swigart (SBN 225557)
josh@swigartlawgroup.com
SWIGART LAW GROUP, APC
2221 Camino Del Rio S., Suite 308
San Diego, CA 92108
Tel: (866) 219-3343; Fax: (866) 219-8344

Ben Travis (SBN 305641)
ben@bentravislaw.com
BEN TRAVIS LAW, APC
4660 La Jolla Village Drive, Suite 100
San Diego, CA 92122
Phone: (619) 353-7966

Additional counsel listed on signature page

Attorneys for Plaintiff Andrew Rose
and the putative class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

ANDREW ROSE, an individual, on behalf of himself and all others similarly situated,

Plaintiff,

v.

AMERITA, INC.,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

CLASS ACTION

Plaintiff ANDREW ROSE ("Plaintiff"), by and through his attorneys, brings this class action on behalf of himself, and the Class, as defined below, against Defendant AMERITA, INC. ("Amerita" or "Defendant"). Plaintiff hereby alleges, on information and belief, except for information based on personal knowledge, which allegations are likely to have evidentiary support after further investigation and discovery, as follows:

INTRODUCTION

1. Plaintiff brings this Class Action because of Defendant's failure to properly secure and safeguard individuals' sensitive personal data.

2. Defendant is a specialty infusion company focused on providing complex pharmaceutical products and clinical services to patients outside of the hospital.

3. Plaintiff and all other persons similarly situated had a right to keep their Personally Identifiable Information ("PII") maintained by Defendant confidential (the PII maintained by Defendant is collectively referred to as "Sensitive Information"). Plaintiff and other members of the Class relied on Defendant to keep their Sensitive Information confidential as required by the applicable laws.

4. Defendant violated this right. It failed to implement or follow reasonable data security procedures as required by law and failed to protect Plaintiff and the proposed Class members' Sensitive Information from unauthorized access.

5. As a result of Defendant's inadequate data security and inadequate or negligent training of its employees, Plaintiff's and other proposed Class members' Sensitive Information, including confidential medical information, was accessed and taken by unauthorized third parties. ("Data Breach").

6. While Defendant learned of the breach on March 13, 2023, it waited till September 2, 2023 to notify Plaintiff and other Class members.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect Plaintiff's and other Class members' Sensitive Information.

8. Defendant disregarded the rights of Plaintiff and Class members by, among other things, recklessly or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have reasonable or adequately robust computer systems and security practices to safeguard Sensitive Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

9. As a result of Defendant's failure to implement and follow reasonable security procedures, Class members' Sensitive Information is now exposed. Plaintiff and Class members have spent, and will continue to spend, significant amounts of time and money trying to protect themselves from the adverse ramifications of the Data Breach and dealing with actual fraud and will forever be at a heightened risk of identity theft and fraud.

10. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for (1) violation of the California Confidentiality of Medical Information Act ("CMIA") (Cal. Civ. Code § 56 *et seq.*); (2) negligence; (3) invasion of privacy; (4) breach of implied contract; (5) breach of fiduciary duty; (6) breach of confidence; (7) violation of the California Unfair Competition Law (Cal. Business & Professions Code § 17200, *et seq.*); (8) violation of the California Customer Records Act ("CCRA") (Cal. Civ. Code § 1798.80, *et seq.*), and (9) violations of the California Consumer Privacy Act ("CCPA") (Cal. Civ. Code § 1798.150, *et seq.*). Plaintiff and the Class members seek damages, including but not limited to nominal damages from Defendant, and to compel Defendant to adopt reasonably sufficient security practices to safeguard Sensitive Information that remains in Defendant's custody to prevent incidents like the Data Breach from reoccurring in the future.

JURISDICTION AND VENUE

11. This Court has personal jurisdiction over Defendant because Defendant

conducts substantial business in California and it is registered to do business in California.

12. This court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. 1332(d), as Plaintiff and Defendant are diverse, there are over 100 Class members, and the amount in controversy exceeds $5 million.

13. Venue is proper in this Court because Defendant employs numerous individuals in this District and a substantial portion of the acts giving rise to this action occurred in this District.

PARTIES

14. Plaintiff is an individual over the age of eighteen years, and at all times relevant herein was and is, a resident of the County of Ventura in the State of California.

15. Defendant is a corporation incorporated in Delaware and has its principal place of business in Kentucky.

FACTUAL ALLEGATIONS

A. Background

16. Defendant is a specialty infusion company focused on providing complex pharmaceutical products and clinical services to patients outside of the hospital.

17. As part of its business, Defendant stores a vast amount of Sensitive Information. In doing so, Defendant was entrusted with, and obligated to safeguard and protect, the Sensitive Information of Plaintiff and the Class in accordance with all applicable laws.

B. The Data Breach

18. On or around September 2, 2023, Defendant issued a Notice of Data Breach notifying consumers of an incident involving unauthorized access to personal information. Defendant provided this Data Breach Notification to an undisclosed number of members ("September 2023 Data Breach Notice"). The September 2023 Data Breach Notice informed the affected members that on March 13, 2023, it learned of suspicious activity on its computer network. And after an internal investigation, it

determined that an unknown third party accessed its computer systems from March 12-13, 2023 and that certain personal information may have been obtained from its systems as part of the incident.

19. The September 2023 Data Breach Notice identified the following data points: name, address, certain patient information, such as medical history, diagnosis, medications and health insurance information.

20. Defendant failed to put in place proper security protocols to protect against the unauthorized release of consumers' information and failed to properly train its employees on such protocols, resulting in the unauthorized release of private data. As a result of Defendant's failures, Plaintiff and the Class members' Sensitive Information was accessed and viewed by unknown and unauthorized third parties and is available on the dark web. This means that the Data Breach was successful: unauthorized individuals accessed Plaintiff's and the Class members' unencrypted, unredacted information set forth above.

21. Plaintiff received the September 2023 Data Breach Notice from Defendant on or about September 2, 2023, informing him of the Data Breach and that his Sensitive Information was present in the affected Amerita systems. The Data Breach notification indicated the following information may have been compromised: name, address, certain patient information, such as medical history, diagnosis, medications and health insurance information.

22. This kind of Sensitive Information is highly valued by criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.

C. Plaintiff's Exposure

23. Knowing that thieves stole his Sensitive Information and knowing that his Sensitive Information may now or in the future be available for sale on the dark web has caused Plaintiff great anxiety. He is now very concerned about fraud and identity

theft.

24. Plaintiff suffered actual injury from having his Sensitive Information exposed as a result of the Data Breach including, but not limited to: (a) damages to and diminution in the value of his Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant; (b) loss of his privacy; (c) imminent and impending injury arising from the increased risk of fraud and identity theft; and (d) the time and expense of mitigation efforts as a result of the Data Breach.

25. As a result of the Data Breach, Plaintiff will continue to be at heightened risk for financial fraud, and identity theft, and the attendant damages, for years to come.

26. Defendant's failure to provide immediate formal notice of the Breach to Plaintiff and Class members exacerbated the injuries resulting from the Breach.

D. Defendant Knew or Should Have Known of the Risk Because Medical Providers are Particularly Susceptible to Cyber Attacks.

27. The number of U.S. data breaches surpassed 1,000 in 2016—a record high and a 40 percent increase in the number of data breaches from the previous year.[1] In 2017, 1,579 breaches were reported—a new record high and a 44.7 percent increase in just one year.[2] That trend continues.

28. Medical information is especially valuable to identity thieves. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the

[1] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html (last accessed September 11, 2023).

[2] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf (last accessed September 11, 2023).

substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

29. Defendant knew and understood that unprotected or exposed Sensitive Information in the custody of medical providers, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Sensitive Information through unauthorized access. Indeed, when compromised, highly confidential related data is among the most sensitive and personally consequential. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impacts the economy as a whole.

30. Defendant knew, or should have known, the importance of safeguarding Sensitive Information entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

E. Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII.

31. Defendant acquires, collects, and stores a massive amount of consumers' protected confidential information and other personally identifiable data.

32. As a condition of providing services, Defendant requires consumers to entrust it with highly confidential Sensitive Information.

33. By requiring, obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Sensitive Information, Defendant assumed legal and equitable duties, and knew or should have known it was responsible for protecting Plaintiff's and Class members' Sensitive Information from disclosure.

34. Plaintiff and Class members have taken reasonable steps to maintain the confidentiality of their Sensitive Information. Plaintiff and Class members relied on Defendant to keep their Sensitive Information confidential and securely maintained, to

use this information for business purposes only, to only allow authorized disclosures of this information, and prevent unauthorized disclosure of the information.

F. The Value of PII and the Effects of Unauthorized Disclosure.

35. Defendant was well aware of the highly private nature of the Sensitive Information it collects and its significant value to those who would use it for wrongful purposes.

36. Sensitive Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can commit an array of crimes including identify theft, medical fraud, and financial fraud.[3] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

37. The ramifications of Defendant's failure to keep Plaintiff's and Class members' Sensitive Information secure are long lasting and severe. Once Sensitive Information is stolen, fraudulent use of that information and damage to victims may continue for years.

38. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Sensitive Information and of the foreseeable consequences if its data security systems were breached, including the significant costs that would be imposed on consumers as a result of a breach.

G. Defendant Failed to Comply with FTC Guidelines.

39. The Federal Trade Commission ("FTC") promulgates numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[4]

---

[3] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed September 11, 2023).

[4] Federal Trade Commission, *Start With Security*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-

40. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[5] The guidelines note that businesses should protect the personal customer information they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

41. The FTC further recommends companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry–tested methods for security; monitor for suspicious activity on the network; and verify third–party service providers have implemented reasonable security measures.[6]

42. The FTC brings enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

43. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

44. Defendant was at all times fully aware of its obligation to protect Plaintiff's

---

startwithsecurity.pdf (last accessed September 11, 2023).

[5] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed September 11, 2023).

[6] FTC, *Start With Security*, *supra.*

and Class members' Sensitive Information because of Defendant's position as a trusted and experienced medical provider. Defendant was also aware of the significant repercussions that would result from its failure to do so.

H. Defendant Failed to Comply with Industry Standards.

45. Defendant failed to implement several basic cybersecurity safeguards that can be implemented to improve cyber resilience and require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of PII; (b) educating and training employees on how to protect PII; and (c) correcting the configuration of software and network devices.

46. Private cybersecurity firms have also identified businesses as being particularly vulnerable to cyber-attacks, both because of the value of the PII they maintain and because employees have been slow to adapt and respond to cybersecurity threats.[7] These private cybersecurity firms have also promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of PII.

47. Despite the abundance and availability of information regarding the threats and cybersecurity best practices to defend against those threats, Defendant chose to ignore them. These best practices were known, or should have been known by Defendant, whose failure to heed and properly implement industry standards directly led to the Data Breach and the unlawful exposure of Sensitive Information.

I. Defendant Failed to Comply with HIPAA.

48. Under the Health Insurance Portability Act of 1996 ("HIPAA") Defendant had a heightened duty to protect patient Private Information.

49. Defendant failed to comply with HIPAA by not:

a. Ensuring the confidentiality and integrity of electronic protected health

[7] Stickman Cyber, *Why Cybersecurity In The Workplace Is Everyone's Responsibility, available at:* https://www.stickmancyber.com/cybersecurity-blog/why-cybersecurity-in-the-workplace-is-everyones-responsibility (last accessed September 11, 2023).

information ("PHI") it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

b. Implementing technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

c. Implementing policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

d. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

e. Protecting against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

f. Protecting against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

g. Ensuring compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or

h. Training all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b).

J. Plaintiff and Class Members Suffered Damages.

50. The ramifications of Defendant's failure to keep Plaintiff's and Class members' Sensitive Information secure are long lasting and severe. Once that kind of Sensitive Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

51. The Sensitive Information belonging to Plaintiff and Class members is private, sensitive in nature, and left inadequately protected by Defendant—who did not obtain Plaintiff's or Class members' consent to disclose such Sensitive Information to any other person as required by applicable law and industry standards.

52. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff's and Class members' Sensitive Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Sensitive Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

53. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect member data.

54. Defendant could have prevented the intrusions into its systems and, ultimately, the theft of Sensitive Information if Defendant had remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field.

55. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members are now in imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to dedicate time and resources which they otherwise would have dedicated to other life demands, such as work and family, to mitigate the actual and potential impact of the Data Breach on their lives.

56. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems," and that "resolving the problems caused by

identity theft may take more than a year for some victims."[8]

57. As a direct result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Sensitive Information;

b. Out–of–pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and loss of productivity from addressing and attempting to mitigate actual and future consequences of the Data Breach, including but not limited to researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their Sensitive Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Sensitive Information in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

58. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring their Sensitive Information is secure, remains secure, and is not subject to further misappropriation and theft.

[8] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed September 11, 2023).

K. Defendant's Delay in Identifying & Reporting the Breach Caused Additional Harm.

59. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[9]

60. Indeed, once a data breach has occurred:

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills, insurance invoices, and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves (internal citations omitted).[10]

61. Although their Sensitive Information was improperly exposed on or about March 13, 2023, Plaintiff and Class members were not notified of the Data Breach until on or about September 2, 2023, depriving Plaintiff and Class members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

---

[9] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire, *available at:* https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last accessed September 11, 2023).

[10] Consumer Reports, *The Data Breach Next Door: Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too*, January 31, 2019, *available at:* https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed September 11, 2023).

62. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, there is an increased risk of fraud for Plaintiff and Class members.

CLASS ACTION ALLEGATIONS

63. Plaintiff brings this class action pursuant to Rule 23(a) and (b)(3) of the Federal Rules of Civil Procedure, on behalf of the following Class and Subclass:

> All individuals whose Sensitive Information stored or possessed by Defendant was subject to the Data Breach (the "Class").
>
> All California residents whose Sensitive Information stored or possessed by Defendant was subject to the Data Breach (the "California Subclass").

64. Excluded from the Class are Defendant, its officers and directors, families and legal representatives, heirs, successors, or assigns and any entity in which Defendant has a controlling interest, and any Judge assigned to this case and their immediate families.

65. Plaintiff reserves the right to amend or modify the definition of the Class and Subclass to provide greater specificity and/or further division into subclasses or limitation to particular issues.

66. **Numerosity- Fed. R. Civ. P. 23(a)(1):** The members of the Class are so numerous that joinder of all members is impracticable. The exact number or identification of class members is presently unknown, but it is believed that there are thousands of class members in the Class. The identities of the Class Members are ascertainable and can be determined based on records maintained by Defendant.

67. **Predominance of Common Questions- Fed R. Civ. P. 23(a)(2), 23(b)(3):** There are multiple questions of law and fact common to the Class that will predominate over questions affecting only individual class members. The questions of fact and law that are common to the Class members and predominate over questions

that may affect individual Class members, include:

a) Whether Plaintiff's and the Class members' Sensitive Information was accessed and/or viewed by one or more unauthorized persons in the Data Breach alleged above;

b) When and how Defendant should have learned and actually learned of the Data Breach;

c) Whether Defendant's response to the Data Breach was adequate;

d) Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their Sensitive Information;

e) Whether Defendant breached that duty;

f) Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class members' Sensitive Information;

g) Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class members' Sensitive Information;

h) Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class members' Sensitive Information secure and prevent loss or misuse of that Sensitive Information;

i) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j) Whether Defendant caused Plaintiff and Class members damages;

k) Whether Defendant violated the law by failing to promptly notify Class members their Sensitive Information was compromised;

l) Whether Plaintiff and Class members are entitled to actual damages, nominal and/or statutory damages, credit monitoring, other monetary relief, and/or equitable relief;

m) Whether Defendant violated the California Unfair Competition Law (Business & Professions Code § 17200, et seq.);

n) Whether Defendant violated the California Customer Records Act (Cal. Civ. Code § 1798.80, et seq.:

o) Whether Defendant violated the California Consumer Privacy Act ("CCPA") (Cal. Civ. Code § 1798.100, et seq.).

68. **Typicality- Fed. R. Civ. P. 23(a)(3):** Plaintiff's claims are typical of those of other Class members because all had their Sensitive Information compromised because of the Data Breach, due to Defendant's virtually identical conduct.

69. **Adequacy—Fed. R. Civ. P. 23(a)(4); 23(g)(1):** Plaintiff is an adequate representative of the Class because he is a member of the Class and his interests do not conflict with the interests of the members of the Class he seeks to represent. Plaintiff is represented by experienced and competent Class Counsel. Class Counsel have litigated numerous class actions. Class counsel intend to prosecute this action vigorously for the benefit of everyone in the Class. Plaintiff and Class Counsel can fairly and adequately protect the interests of all of the members of the Class.

70. **Superiority—Fed. R. Civ. P. 23(b)(3):** The class action is superior to other available methods for fairly and efficiently adjudicating this controversy because individual litigation of Class members' claims would be impracticable and individual litigation would be unduly burdensome to the courts. Without the class action vehicle, the Class would have no reasonable remedy and would continue to suffer losses. Further, individual litigation has the potential to result in inconsistent or contradictory judgments. There is no foreseeable difficulty in managing this action as a class action and it provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

First Cause of Action

Violation of California's Confidentiality of Medical Information Act ("CMIA")
(Cal. Civ. Code § 56, et seq.)
[On Behalf of Plaintiff and the California Subclass]

71. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

72. Defendant is a "provider of healthcare," as defined in Cal. Civ. Code § 56.06 and/or a "contractor," and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

73. Plaintiff and the Class are "patients," as defined in the CMIA, Cal. Civ. Code § 56.05(l) ("'Patient' means a natural person, whether or not still living, who received health care services from a provider of healthcare and to whom medical information pertains.").

74. Defendant disclosed "medical information," as defined in the CMIA, Cal. Civ. Code § 56.05(i), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the inactions of Defendant, including its failure to adequately implement sufficient data security measures and protocols to protect Plaintiff's and Class members' personal and medical information, which allowed unauthorized individuals to obtain Plaintiff's and the Class members' medical information.

75. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff and the Class to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and Class members' medical information in a manner that preserved the confidentiality of the information contained therein, was in violation of Cal. Civ. Code §§ 56.06 and

56.101(a).

76. Defendant's systems and protocols did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A).

77. Plaintiff and the Class were injured and have suffered damages, as described above, from Defendant's illegal disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

Second Cause of Action

Negligence

[On Behalf of Plaintiff and the Class]

78. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

79. Defendant's own negligent conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendant's negligence included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's negligence also included its decision not to comply with (1) industry standards, and/or best practices for the safekeeping and encrypted authorized disclosure of the Sensitive Information of Plaintiff and Class members; or (2) Section 5 of the FTC Act.

80. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing its security protocols to ensure Sensitive Information in Defendant's possession was adequately secured and protected, and

that employees tasked with maintaining such information were adequately trained on relevant cybersecurity measures. Defendant also had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiff's and Class members' Sensitive Information.

81. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

82. Plaintiff and the Class members entrusted their Sensitive Information to Defendant with the understanding that Defendant would safeguard their information.

83. Defendant was in a position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach. However, Plaintiff and Class members had no ability to protect their Sensitive Information in Defendant's possession.

84. Defendant had full knowledge of the sensitivity of the Sensitive Information, and the types of harm Plaintiff and Class members could, would, and will suffer if the Sensitive Information were wrongfully disclosed.

85. Plaintiff and Class members were the foreseeable and probable victims of Defendant's negligent and inadequate security practices and procedures that led to the Data Breach. Defendant knew or should have known of the inherent risks in collecting and storing the highly valuable Sensitive Information of Plaintiff and Class members, the critical importance of providing adequate security of that Sensitive Information, the current cyber security risks being perpetrated, and that Defendant had inadequate employee training, monitoring and education and IT security protocols in place to secure the Sensitive Information of Plaintiff and Class members.

86. Defendant negligently, through its actions and/or omissions, and unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class members' Sensitive Information while the data was within Defendant's possession and/or control by failing to comply with and/or deviating from standard industry rules, regulations, and practices at the time of the Data Breach.

87. The harm the Data Breach caused is the type of harm privacy laws were intended to guard against. And Plaintiff and Class members are within the class of persons privacy laws were intended to protect.

88. Defendant negligently failed to comply with privacy laws by failing to protect against and prevent the dissemination of Plaintiff's and Class members' Sensitive Information to unauthorized third parties.

89. Defendant's violations of Section 5 of the FTC Act also constitute negligence. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Sensitive Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

90. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class members' Sensitive Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information it required, obtained, and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class members.

91. Plaintiff and Class members are within the class of persons the FTC Act was intended to protect.

92. The harm the Data Breach caused, and continues to cause, is the type of

harm the FTC Act was intended to guard against. The FTC pursues enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class members.

93. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of Plaintiff's and Class members' Sensitive Information.

94. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff and Class members the existence and scope of the Data Breach.

95. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class members, Plaintiff's and Class members' Sensitive Information would not have been compromised.

96. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the Sensitive Information and the harm suffered, and/or risk of imminent harm suffered, by Plaintiff and Class members.

97. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered, and continue to suffer, injuries and damages arising from the Data Breach, including, but not limited to: damages from lost time and efforts to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months—if not years—to discover, detect, and remedy.

98. Additionally, as a direct and proximate result of Defendant's negligence,

Plaintiff and Class members have suffered, and will continue to suffer, the continued risks of exposure of their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession.

Third Cause of Action

Invasion of Privacy

[On Behalf of Plaintiff and the Class]

99. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

100. Plaintiff and Class members had a legitimate expectation of privacy with respect to their Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

101. Defendant owed a duty to its members, including Plaintiff and Class members, to keep their Sensitive Information confidential.

102. The unauthorized release of Sensitive Information, especially medical information, is highly offensive to a reasonable person.

103. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class members disclosed their Sensitive Information to Defendant, but privately, with the intention that the Sensitive Information would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

104. The Data Breach constitutes an intentional interference with Plaintiff's and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

105. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

106. Acting with knowledge, Defendant had notice and knew its inadequate cybersecurity practices would cause injury to Plaintiff and Class members.

107. As a proximate result of Defendant's acts and omissions, Plaintiff and Class members' Sensitive Information was disclosed to, and used by, third parties without authorization, causing Plaintiff and Class members to suffer damages.

108. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class members in that the Sensitive Information maintained by Defendant may be breached again—leading to further viewing, distributing, and use of updated and additional Sensitive Information by unauthorized persons.

109. Plaintiff and Class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class members.

Fourth Cause of Action

Breach of Implied Contract

[On Behalf of Plaintiff and the Class]

110. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

111. Defendant solicited and invited Class members to provide their Sensitive Information as part of Defendant's regular business practices. Plaintiff and Class members provided their Sensitive Information to Defendant.

112. In so doing, Plaintiff and Class members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely detect any breaches of their Sensitive Information. In entering into such implied contracts, Plaintiff and Class members reasonably believed

and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

113. Implicit in the agreement between Plaintiff and Class members on the one hand, and the Defendant on the other, regarding providing protected Sensitive Information, was Defendant's obligation to: (a) use such Sensitive Information for business purposes only; (b) take reasonable steps to safeguard that Sensitive Information; (c) prevent unauthorized disclosures of the Sensitive Information; (d) provide Plaintiff and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information; (e) reasonably safeguard and protect the Sensitive Information of Plaintiff and Class members from unauthorized disclosure or uses; and (f) retain the Sensitive Information only under conditions that kept such information secure and confidential.

114. Without such implied contracts, Plaintiff and Class members would not have provided their Sensitive Information to Defendant.

115. Plaintiff and Class members fully performed their obligations under the implied contract with Defendant. However, Defendant did not.

116. Defendant breached the implied contracts with Plaintiff and Class members by failing to:

a. Reasonably safeguard and protect Plaintiff's and Class members' Sensitive Information, which was compromised as a result of the Data Breach; and

b. Identify and respond to suspected or known security incidents.

117. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class members have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying

financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months if not years to discover, detect, and remedy.

Fifth Cause of Action

Breach of Fiduciary Duty

[On Behalf of Plaintiff and the Class]

118. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

119. In light of their special relationship, Defendant became the guardian of Plaintiff's and Class members' Sensitive Information. Defendant became a fiduciary, created by its undertaking and guardianship of Plaintiff's and Class members' Sensitive Information, to act primarily for the benefit of Plaintiff and Class members. This duty included the obligation to safeguard Plaintiff's and Class members' Sensitive Information, and to timely notify them in the event of a data breach.

120. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its relationship. Defendant breached its fiduciary duties owed to Plaintiff and Class members by failing to:

a. Properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class members' protected confidential information and other Sensitive Information;

b. Timely notify and/or warn Plaintiff and Class members of the Data Breach; and

c. Otherwise failing to safeguard Plaintiff's and Class members' Sensitive Information.

121. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered, and will suffer, injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity to control

how their Sensitive Information is used; (c) the compromise, publication, and/or theft of their Sensitive Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (e) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Sensitive Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

122. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class members have suffered, and will continue to suffer, other forms of injury and/or harm, and other economic and non–economic losses.

Sixth Cause of Action

Breach of Confidence

[On Behalf of Plaintiff and the Class]

123. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

124. At all times during Plaintiff's and Class members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class members' Sensitive Information that Plaintiff and Class members provided to Defendant.

125. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class members' Sensitive Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

126. Plaintiff and Class members provided their respective Sensitive Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Sensitive Information to be disseminated to any unauthorized parties.

127. Plaintiff and Class members also provided their Sensitive Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Sensitive Information from unauthorized disclosure, such as following basic principles of protecting its networks and data systems, including Defendant's employees' systems.

128. Defendant required and voluntarily received, in confidence, Plaintiff's and Class members' Sensitive Information with the understanding that the Sensitive Information would not be disclosed or disseminated to the public or any unauthorized third parties.

129. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class members' Sensitive Information, Plaintiff's and Class members' Sensitive Information was disclosed to, and misappropriated by, unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

130. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class members have suffered, and will continue to suffer damages.

131. But for Defendant's disclosure of Plaintiff's and Class members' Sensitive Information in violation of the parties' understanding of confidence, Plaintiff's and Class members' Sensitive Information would not have been

compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class members' Sensitive Information, as well as the resulting damages.

132. The injury and harm Plaintiff and Class members suffered, and continue to suffer, was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class members' Sensitive Information. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class members' Sensitive Information had numerous security and other vulnerabilities placing Plaintiff's and Class members' Sensitive Information in jeopardy.

133. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their Sensitive Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (g) the diminished value of Defendant's services they received.

134. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non–economic losses.

Seventh Cause of Action

Violation of the California Unfair Competition Law,

Cal. Bus. & Prof. Code § 17200, *et seq*.--Unfair Business Practices

[On Behalf of Plaintiff and the California Subclass]

135. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

136. Defendant violated Cal. Bus. & Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair, or fraudulent business acts and practices, that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code § 17200.

137. Defendant engaged in unlawful and unfair acts and practices by establishing the sub–standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Class members' Sensitive Information with knowledge the information would not be adequately protected; and by storing Plaintiff's and Class members' Sensitive Information in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods of safeguarding the Sensitive Information of Plaintiff and Class members.

138. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

139. Defendant also engaged in unlawful acts by violating the privacy and security of HIPAA, 42 U.S.C. §1302d, et seq. and by violating the CMIA, Cal. Civ. Code § 56, et seq.

140. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities that solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, et seq., and the CMIA, Cal. Civ. Code § 56, et seq.

141. As a direct and proximate result of Defendant's unlawful and unfair practices and acts, Plaintiff and Class members were injured and lost money or property, including but not limited to the loss of Plaintiff's and Class members' legally protected interest in the confidentiality and privacy of their Sensitive Information, nominal damages, and additional losses as described herein.

142. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class members' Sensitive Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above–named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class members.

143. Plaintiff, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Class members of money or property Defendant may have acquired by means of Defendant's unlawful, and unfair business practices, restitutionary disgorgement of all monies that accrued to Defendant because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

Eighth Cause of Action

Violation of the California Customer Records Act ("CCRA")

Cal. Civ. Code § 1798.80, *et seq*.

[On Behalf of Plaintiff and the California Subclass]

144. Plaintiff re-alleges and incorporates by reference each and every

allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

145. Section 1798.82 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay."

146. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (Cal. Civ. Code § 1798.82(b).)

147. Any person or business required to issue a security breach notification under the CCRA shall meet the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

iii. If the information is possible to determine at the time the notice is provided, then any of the following:

1. The date of the breach;

2. The estimated date of the breach; or
3. The date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

vi. The toll–free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

148. The Data Breach described herein constituted a "breach of the security system" of Defendant.

149. As alleged above, Defendant unreasonably delayed informing Plaintiff and Class members about the Data Breach, affecting their Sensitive Information, after Defendant knew the Data Breach had occurred.

150. Defendant failed to disclose to Plaintiff and Class members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Sensitive Information when Defendant knew or reasonably believed such information had been compromised.

151. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

152. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff and Class members would impede its investigation.

153. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class members were deprived of prompt notice of the Data Breach, and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and Class members because their stolen information would have had less value to identity thieves.

154. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and Class members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

155. Plaintiff and Class members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiff and Class members as alleged above and equitable relief.

Ninth Cause of Action

Violation of the California Consumer Privacy Act ("CCPA")

Cal. Civ. Code § 1798.150, *et seq*.

[On Behalf of Plaintiff and the California Subclass]

156. Plaintiff re-alleges and incorporates by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

157. Defendant is a corporation organized and operated for profit or financial benefit of its owners with annual gross revenues of more than $25 million. Defendant collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

158. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and Class members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

159. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and Class members' PII. As detailed herein, Defendant failed to do so. As a direct and proximate result of Defendant's acts, Plaintiff's and Class members' PII were subjected to unauthorized access and exfiltration, theft or disclosure.

160. Plaintiff and Class members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards consumers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold consumers' PII including Plaintiff's and Class members' PII. Plaintiff and Class members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

1. That the Court certify this action as a Class Action under FRCP 23 and appoint Plaintiff as representative of the Class and his attorneys as Class Counsel;
2. Granting injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:
    i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein,
    ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws,
    iii. requiring Defendant to delete, destroy, and purge the personal

information of Plaintiff and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members,

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal information of Plaintiff and Class members' personal information,

v. prohibiting Defendant from maintaining Plaintiff's and Class members' personal information on a cloud-based database,

vi. requiring Defendant to engage independent 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, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors,

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring,

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures,

ix. requiring Defendant to conduct regular database scanning and securing checks,

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal information, as well as protecting the

personal information of Plaintiff and Class members,

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal information,

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated,

xiv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal information to third parties, as well as the steps affected individuals must take to protect themselves,

xv. requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected,

xvi. requiring Defendant to disclose any future data disclosures in a timely and accurate manner; and

xvii. requiring Defendant to provide ongoing credit monitoring and identity theft repair services to Class members.

3. An award of compensatory, statutory, and nominal damages in an amount to

be determined;

4. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
5. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and
6. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all claims so triable.

DATED: September 25, 2023

LOKER LAW, APC

/s/ Matthew M. Loker
Matthew M. Loker
Attorneys for Plaintiff

ClassAction.org
