

1 Joshua B. Swigart (SBN 225557)
2 *josh@swigartlawgroup.com*
3 **SWIGART LAW GROUP, APC**
4 2221 Camino Del Rio S., Suite 308
5 San Diego, CA 92108
6 Tel: (866) 219-3343; Fax: (866) 219-8344

7 Ben Travis (SBN 305641)
8 *ben@bentravislaw.com*
9 **BEN TRAVIS LAW, APC**
10 4660 La Jolla Village Drive, Suite 100
11 San Diego, CA 92122
12 Phone: (619) 353-7966

13 *Additional counsel listed on signature page*

14 Attorneys for Plaintiff Andrew Rose
15 and the putative class

16 **UNITED STATES DISTRICT COURT**
17 **CENTRAL DISTRICT OF CALIFORNIA**

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

21 Plaintiff,

22 v.

23 AMERITA, INC.,

24 Defendant.

25 Case No.:

26 **CLASS ACTION COMPLAINT**

27 **DEMAND FOR JURY TRIAL**

28 **CLASS ACTION**

1
2 Plaintiff ANDREW ROSE (“Plaintiff”), by and through his attorneys, brings this
3 class action on behalf of himself, and the Class, as defined below, against Defendant
4 AMERITA, INC. (“Amerita” or “Defendant”). Plaintiff hereby alleges, on information
5 and belief, except for information based on personal knowledge, which allegations are
6 likely to have evidentiary support after further investigation and discovery, as follows:

7 **INTRODUCTION**

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

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

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

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

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

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

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

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

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

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

9 **PARTIES**

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

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

14 **FACTUAL ALLEGATIONS**

15 **A. Background**

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

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

22 **B. The Data Breach**

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

1 determined that an unknown third party accessed its computer systems from March 12-
2 13, 2023 and that certain personal information may have been obtained from its systems
3 as part of the incident.

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

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

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

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

25 **C. Plaintiff's Exposure**

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

1 theft.

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

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

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

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

14 27. The number of U.S. data breaches surpassed 1,000 in 2016—a record high
15 and a 40 percent increase in the number of data breaches from the previous year.¹ In
16 2017, 1,579 breaches were reported—a new record high and a 44.7 percent increase in
17 just one year.² That trend continues.

18 28. Medical information is especially valuable to identity thieves. Because of
19 its value, the medical industry has experienced disproportionately higher numbers of
20 data theft events than other industries. Defendant knew or should have known this and
21 strengthened its data systems accordingly. Defendant was put on notice of the
22

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

27 ² Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*,
28 available at:

[https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreach](https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf)
[YearEndReview.pdf](https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf) (last accessed September 11, 2023).

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

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

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

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

17 **PII.**

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

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

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

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

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

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

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

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

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

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

20 **G. Defendant Failed to Comply with FTC Guidelines.**

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

25
26 ³ Federal Trade Commission, *Warning Signs of Identity Theft*, available at:
27 <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last
28 accessed September 11, 2023).

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

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

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

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

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

23 44. Defendant was at all times fully aware of its obligation to protect Plaintiff’s
24

25 [startwithsecurity.pdf](#) (last accessed September 11, 2023).

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

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

4 **H. Defendant Failed to Comply with Industry Standards.**

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

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

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

21 **I. Defendant Failed to Comply with HIPAA.**

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

24 49. Defendant failed to comply with HIPAA by not:

- 25 a. Ensuring the confidentiality and integrity of electronic protected health
26

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

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

- 3 b. Implementing technical policies and procedures for electronic information
4 systems that maintain electronic PHI to allow access only to those persons
5 or software programs that have been granted access rights in violation of
6 45 C.F.R. § 164.312(a)(1);
- 7 c. Implementing policies and procedures to prevent, detect, contain, and
8 correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- 9 d. Implementing procedures to review records of information system activity
10 regularly, such as audit logs, access reports, and security incident tracking
11 reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- 12 e. Protecting against reasonably anticipated threats or hazards to the security
13 or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- 14 f. Protecting against reasonably anticipated uses or disclosures of electronic
15 PHI that are not permitted under the privacy rules regarding individually
16 identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- 17 g. Ensuring compliance with HIPAA security standard rules by their
18 workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or
- 19 h. Training all members of its workforce effectively on the policies and
20 procedures regarding PHI as necessary and appropriate for the members
21 of its workforce to carry out its functions and to maintain security of PHI,
22 in violation of 45 C.F.R. § 164.530(b).

23 **J. Plaintiff and Class Members Suffered Damages.**

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

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

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

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

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

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

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

1 identity theft may take more than a year for some victims.”⁸

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

- 5 a. The compromise, publication, theft and/or unauthorized use of their
6 Sensitive Information;
- 7 b. Out-of-pocket costs associated with the prevention, detection, recovery,
8 and remediation from identity theft or fraud;
- 9 c. Lost opportunity costs and lost wages associated with efforts expended
10 and loss of productivity from addressing and attempting to mitigate actual
11 and future consequences of the Data Breach, including but not limited to
12 researching how to prevent, detect, contest, and recover from identity theft
13 and fraud;
- 14 d. The continued risk to their Sensitive Information, which remains in the
15 possession of Defendant and is subject to further breaches so long as
16 Defendant fails to undertake appropriate measures to protect the Sensitive
17 Information in its possession; and
- 18 e. Current and future costs in terms of time, effort, and money that will be
19 expended to prevent, detect, contest, remediate, and repair the impact of
20 the Data Breach for the remainder of the lives of Plaintiff and Class
21 members.

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

25
26
27 _____
28 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).

1 **K. Defendant’s Delay in Identifying & Reporting the Breach Caused**
2 **Additional Harm.**

3 59. It is axiomatic that:

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

10 60. Indeed, once a data breach has occurred:

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

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

23 ⁹ *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16*
24 *Percent According to New Javelin Strategy & Research Study*, Business Wire,
25 *available at:*

26 <https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million> (last accessed September 11, 2023).

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

1 that may affect individual Class members, include:

- 2 a) Whether Plaintiff's and the Class members' Sensitive Information was
3 accessed and/or viewed by one or more unauthorized persons in the Data
4 Breach alleged above;
- 5 b) When and how Defendant should have learned and actually learned of the
6 Data Breach;
- 7 c) Whether Defendant's response to the Data Breach was adequate;
- 8 d) Whether Defendant owed a duty to the Class to exercise due care in
9 collecting, storing, safeguarding and/or obtaining their Sensitive
10 Information;
- 11 e) Whether Defendant breached that duty;
- 12 f) Whether Defendant implemented and maintained reasonable security
13 procedures and practices appropriate to the nature of storing Plaintiff's
14 and Class members' Sensitive Information;
- 15 g) Whether Defendant acted negligently in connection with the monitoring
16 and/or protecting of Plaintiff's and Class members' Sensitive Information;
- 17 h) Whether Defendant knew or should have known that it did not employ
18 reasonable measures to keep Plaintiff's and Class members' Sensitive
19 Information secure and prevent loss or misuse of that Sensitive
20 Information;
- 21 i) Whether Defendant adequately addressed and fixed the vulnerabilities
22 which permitted the Data Breach to occur;
- 23 j) Whether Defendant caused Plaintiff and Class members damages;
- 24 k) Whether Defendant violated the law by failing to promptly notify Class
25 members their Sensitive Information was compromised;
- 26 l) Whether Plaintiff and Class members are entitled to actual damages,
27 nominal and/or statutory damages, credit monitoring, other monetary
28 relief, and/or equitable relief;

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

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

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

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

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

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

26
27
28

1 **First Cause of Action**

2 **Violation of California’s Confidentiality of**
3 **Medical Information Act (“CMIA”)**
4 **(Cal. Civ. Code § 56, et seq.)**
5 **[On Behalf of Plaintiff and the California Subclass]**

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

8 72. Defendant is a “provider of healthcare,” as defined in Cal. Civ. Code §
9 56.06 and/or a “contractor,” and is therefore subject to the requirements of the CMIA,
10 Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

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

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

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

1 56.101(a).

2 76. Defendant's systems and protocols did not protect and preserve the
3 integrity of electronic medical information in violation of Cal. Civ. Code §
4 56.101(b)(1)(A).

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

11 **Second Cause of Action**

12 **Negligence**

13 **[On Behalf of Plaintiff and the Class]**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6 **Third Cause of Action**

7 **Invasion of Privacy**

8 **[On Behalf of Plaintiff and the Class]**

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

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

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

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

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

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

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

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

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

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

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

16 **Fourth Cause of Action**

17 **Breach of Implied Contract**

18 **[On Behalf of Plaintiff and the Class]**

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

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

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

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

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

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

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

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

- 19 a. Reasonably safeguard and protect Plaintiff's and Class members'
20 Sensitive Information, which was compromised as a result of the Data
21 Breach; and
22 b. Identify and respond to suspected or known security incidents.

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

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

4 **Fifth Cause of Action**

5 **Breach of Fiduciary Duty**

6 **[On Behalf of Plaintiff and the Class]**

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

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

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

- 19 a. Properly encrypt and otherwise protect the integrity of the system
20 containing Plaintiff's and Class members' protected confidential
21 information and other Sensitive Information;
- 22 b. Timely notify and/or warn Plaintiff and Class members of the Data
23 Breach; and
- 24 c. Otherwise failing to safeguard Plaintiff's and Class members' Sensitive
25 Information.

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

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

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

18 **Sixth Cause of Action**

19 **Breach of Confidence**

20 **[On Behalf of Plaintiff and the Class]**

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

24 124. At all times during Plaintiff's and Class members' interactions with
25 Defendant, Defendant was fully aware of the confidential and sensitive nature of
26 Plaintiff's and Class members' Sensitive Information that Plaintiff and Class
27 members provided to Defendant.
28

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

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

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

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

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

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

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

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

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

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

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

4 **Seventh Cause of Action**

5 **Violation of the California Unfair Competition Law,**
6 **Cal. Bus. & Prof. Code § 17200, *et seq.*--Unfair Business Practices**
7 **[On Behalf of Plaintiff and the California Subclass]**

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

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

14 137. Defendant engaged in unlawful and unfair acts and practices by
15 establishing the sub-standard security practices and procedures described herein; by
16 soliciting and collecting Plaintiff’s and Class members’ Sensitive Information with
17 knowledge the information would not be adequately protected; and by storing
18 Plaintiff’s and Class members’ Sensitive Information in an unsecure electronic
19 environment in violation of California’s data breach statute, Cal. Civ. Code §
20 1798.81.5, which requires Defendant to take reasonable methods of safeguarding the
21 Sensitive Information of Plaintiff and Class members.

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

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

28

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

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

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

17 143. Plaintiff, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code
18 § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Class
19 members of money or property Defendant may have acquired by means of
20 Defendant’s unlawful, and unfair business practices, restitutionary disgorgement of
21 all monies that accrued to Defendant because of Defendant’s unlawful and unfair
22 business practices, declaratory relief, attorneys’ fees and costs (pursuant to Cal. Code
23 Civ. Proc. § 1021.5), and injunctive or other equitable relief.

24 **Eighth Cause of Action**

25 **Violation of the California Customer Records Act (“CCRA”)**

26 **Cal. Civ. Code § 1798.80, *et seq.***

27 **[On Behalf of Plaintiff and the California Subclass]**

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

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

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

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

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

- 19 a. The security breach notification shall be written in plain language;
- 20 b. The security breach notification shall include, at a minimum, the
21 following information:
- 22 i. The name and contact information of the reporting person or
23 business subject to this section;
 - 24 ii. A list of the types of personal information that were or are
25 reasonably believed to have been the subject of a breach;
 - 26 iii. If the information is possible to determine at the time the
27 notice is provided, then any of the following:
 - 28 1. The date of the breach;

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

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

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

13 **Ninth Cause of Action**

14 **Violation of the California Consumer Privacy Act (“CCPA”)**

15 **Cal. Civ. Code § 1798.150, *et seq.***

16 **[On Behalf of Plaintiff and the California Subclass]**

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

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

23 158. Defendant violated § 1798.150 of the CCPA by failing to prevent
24 Plaintiff’s and Class members’ nonencrypted PII from unauthorized access and
25 exfiltration, theft, or disclosure as a result of Defendant’s violations of its duty to
26 implement and maintain reasonable security procedures and practices appropriate to
27 the nature of the information.
28

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

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

13 **PRAYER FOR RELIEF**

14 **WHEREFORE**, Plaintiff prays for judgment as follows:

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

- 1 information of Plaintiff and Class members unless Defendant can
2 provide to the Court reasonable justification for the retention and
3 use of such information when weighed against the privacy
4 interests of Plaintiff and Class members,
- 5 iv. requiring Defendant to implement and maintain a comprehensive
6 Information Security Program designed to protect the
7 confidentiality and integrity of the personal information of
8 Plaintiff and Class members' personal information,
- 9 v. prohibiting Defendant from maintaining Plaintiff's and Class
10 members' personal information on a cloud-based database,
- 11 vi. requiring Defendant to engage independent third-party security
12 auditors/penetration testers as well as internal security personnel
13 to conduct testing, including simulated attacks, penetration tests,
14 and audits on Defendant's systems on a periodic basis, and
15 ordering Defendant to promptly correct any problems or issues
16 detected by such third-party security auditors,
- 17 vii. requiring Defendant to engage independent third-party security
18 auditors and internal personnel to run automated security
19 monitoring,
- 20 viii. requiring Defendant to audit, test, and train its security personnel
21 regarding any new or modified procedures,
- 22 ix. requiring Defendant to conduct regular database scanning and
23 securing checks,
- 24 x. requiring Defendant to establish an information security training
25 program that includes at least annual information security training
26 for all employees, with additional training to be provided as
27 appropriate based upon the employees' respective responsibilities
28 with handling personal information, as well as protecting the

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- 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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- 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