

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

M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829
Email: aberry@justice4you.com

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
401 W Broadway, Suite 1760
San Diego, CA 92101
Tel.: (858) 209-6941
jnelson@milberg.com

Attorneys for Plaintiff and the Proposed Class

**SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF SAN DIEGO**

MICHAEL WILSON, a person lacking legal capacity, by MOSANTHONY WILSON, his conservator, on behalf of himself and all others similarly situated,

Plaintiff,

v.

MAXIM HEALTHCARE SERVICES, INC., a Maryland Corporation,

Defendant.

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego
11/16/2022 at 01:49:15 PM
Clerk of the Superior Court
By Taylor Crandall, Deputy Clerk

Case No. 37-2022-00046497-CU-MC-CTL

CLASS ACTION COMPLAINT FOR DAMAGES, INJUNCTIVE AND EQUITABLE RELIEF FOR:

1. VIOLATIONS OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT

DEMAND FOR JURY TRIAL

1 Plaintiff Michael Wilson, a person lacking legal capacity, by Mosanthony Wilson, his
2 conservator (“Plaintiff”), individually and on behalf of all others similarly situated, by and
3 through his undersigned counsel, brings this action against Defendant Maxim Healthcare
4 Services, Inc. (“Defendant” or “Maxim”), to hold Defendant accountable for the harm it caused
5 Plaintiff and similarly situated individuals (“Class Members”) due to its failure to take reasonable
6 precautions to protect the confidential medical information and sensitive personal information
7 that it collects and maintains in the regular course of business from unauthorized and unlawful
8 access, use or disclosure. In support hereof, Plaintiff alleges, upon personal knowledge as to his
9 own actions and his counsels’ investigations, and upon information and belief as to all other
10 matters, as follows:

11
12 **SUMMARY OF THE ACTION**

13
14 1. Maxim is a national provider of health care services. Through its 147 locations
15 nationwide, Defendant offers a comprehensive set of skilled nursing, physical rehabilitation,
16 companion care, respite care, and behavioral care for individuals with chronic and acute illnesses
17 and disabilities. Due to the nature of Defendant’s business, it collects, maintains, or disposes of
18 confidential patient information, including personally identifiable information (“PII”) and
19 protected health information (“PHI”) (collectively, “Private Information”).¹

20
21 2. Plaintiff and members of the putative class are current and former Maxim patients
22 whose Private Information was accessed by an unauthorized malicious actor because Defendant
23

24 ¹ As used in this Complaint, personally identifiable information (“PII”) generally refers to information that alone or
25 in conjunction with other information identifies an individual, including an individual’s contact information
26 (including postal addresses, email addresses, and phone numbers), Social Security number (SSNs), date of birth,
27 driver’s license number or government-issued identification number, financial account numbers. See generally Cal.
28 Civ. Code § 1798.80, Cal. Civ. Code § 1798.82, 2 C.F.R. § 200.79. Personal health information (“PHI”) is a
category of information that relates to an individual’s physical or mental health and the provision of health care.
Among other things, as used in this complaint PHI includes medical information as that term is defined in Cal. Civ.
Code § 56.05, namely “any individually identifiable information, in electronic or physical form, in possession of or
derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a
patient’s medical history, mental or physical condition, or treatment.”

1 failed to establish reasonable and adequate security practices to safeguard the confidentiality of
2 the patient information Maxim creates, maintains, preserves, stores, abandons, destroys, or
3 disposes.

4 3. On or about November 4, 2021, Defendant announced a breach of its information
5 system's security that compromised Plaintiff's and the Class's Private Information (the "Data
6 Breach"). Defendant's investigation revealed that a malicious actor gained access to Maxim
7 employees' email accounts between October 1, 2020 and December 4, 2020, thereby gaining
8 access to emails and attachments containing patients' Private Information, including names,
9 addresses, dates of birth, contact information, medical history, medical condition or treatment
10 information, medical record number, diagnosis code, patient account number, Medicare/Medicaid
11 number, username/password, and Social Security numbers ("SSNs"). According to public
12 records, the Data Breach affected at least 65,267 people.

14 4. The Data Breach was preventable and a direct result of Defendant's failure to
15 implement adequate and reasonable cybersecurity procedures and protocols necessary to protect
16 its patients' Private Information.

18 5. Additionally, Defendant waited at least 335 days *before beginning to mail*
19 *notification letters* to Plaintiff and the Class of the Data Breach and notifying the regulatory
20 authorities in violation of its legal data breach notification duties.

21 6. Defendant disregarded Plaintiff's and Class Members' rights by, among other
22 things, intentionally, willfully, recklessly, or negligently failing to take and implement adequate
23 and reasonable measures to ensure that Plaintiff's and Class Members' Private Information stored
24 within Defendant's information system were protected and safeguarded against unauthorized
25 access, misuse, and disclosure, failing to take basic industry-standard steps to prevent, identify,
26 contain a breach of its system's security, failing to follow applicable, required and appropriate
27

1 protocols, policies and procedures regarding the encryption of data, even for internal use, and
2 failing to give timely and adequate notice to Plaintiff and Class Members that their Private
3 Information had been subject to the unauthorized access of an unknown third party.

4 7. As a result of Defendant's conduct, Plaintiff's and Class Members' Private
5 Information is now in the hands of, and has been viewed by, an unknown and unauthorized third
6 party.

7 8. Plaintiff and Class Members have lost the confidentiality and control over their
8 Private Information.

9 9. Plaintiff, on behalf of all others similarly situated, alleges a claim for violation of
10 the Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq.*).

11 10. Plaintiff and Class Members seek all available remedies, including but not limited
12 to, statutory and nominal damages, compensatory damages for identity theft, fraud, and time
13 spent, reimbursement of out-of-pocket costs, adequate credit monitoring services funded by
14 Defendant, and injunctive relief including improvements to Defendant's data security systems
15 and practices to ensure they have reasonably sufficient security practices to safeguard patients'
16 Private Information that remains in Defendant's custody to prevent incidents like the Data Breach
17 from reoccurring in the future.

20 **PARTIES**

21 **A. Plaintiff**

22 11. Plaintiff Michael Wilson is, and at all times relevant to this action has been, a
23 resident of San Diego, County of San Diego, California. Plaintiff Wilson suffers from autism,
24 severe epilepsy and other medical conditions and has received in-home medical care from
25 Defendant since approximately 2015. On or about November 4, 2021, Plaintiff Wilson received
26

1 notice from Defendant that his Private Information was compromised in the Data Breach,
2 including his treatment information, medical record number, and patient account number.

3 12. Conservator Mosanthony Wilson is a resident of the State of California and is the
4 parent of his adult disabled child, Plaintiff Michael Wilson. In or about 2013, on application made
5 on Plaintiff Wilson's behalf, Mosanthony Wilson was appointed by the state of California as his
6 son's conservator and has routinely qualified as such ever since.

7
8 **B. Defendant**

9 13. Defendant Maxim Healthcare Services, Inc. is a Maryland corporation
10 headquartered at 7227 Lee Deforest Drive, Columbia, MD 21046.

11 14. Relevant to this action, Defendant transacts business in California, and
12 Defendant's health care services to Plaintiff Wilson and the proposed class were offered out of its
13 facilities in San Diego and throughout California.

14 15. Whenever in this Complaint it is alleged that Defendant did any act, it is meant
15 that the named Defendant performed or participated in the act, or the named Defendant's officers,
16 agents, partners, trustees, or employees performed or participated in the act on behalf of and under
17 the authority of the Defendant. All of the claims stated in this petition are asserted against
18 Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.
19

20 **JURISDICTION AND VENUE**

21 16. This Court has jurisdiction over Plaintiff and Class Members' claims for damages
22 and injunctive relief pursuant to Cal. Civ. Code § 56, *et seq.*, § 1798, *et seq.*, and Cal. Bus. &
23 Prof. Code § 17200, *et seq.*, among other California state statutes. This action is brought as a class
24 action on behalf of Plaintiffs and the Class members pursuant to Cal. Code Civ. Proc. § 382.
25

26 17. Venue is proper in this Court under California Code of Civil Procedure §§ 395(a)
27 and 395.5 and California Bus. & Prof. Code § 17203 because Plaintiff resides in this judicial
28

1 district, Defendant provided the aforementioned services within this County to numerous Class
2 Members and transacts business, has agents, and is otherwise within this Court’s jurisdiction for
3 purposes of service of process. Additionally, and a substantial part of the events or omissions
4 giving rise to Plaintiff’s claims occurred in this judicial district. The unlawful acts alleged in this
5 complaint have had a direct effect on Plaintiff and those similarly situated within the State of
6 California and within this County.

7 8 **STATEMENT OF FACTS**

9 **A. Defendant’s Business Practices**

10 18. Maxim is a national health care provider offering skilled nursing, physical
11 rehabilitation, companion care, respite care, and behavioral care for individuals with chronic and
12 acute illnesses and disabilities.²

13 19. Due to the nature of its services, Defendant collects PII and PHI. Defendant uses
14 the Private Information it collects to create and maintain records stored in digital format on
15 hardware, such as computers, mobile devices, flash drives, off-site “clouds” or similar storage
16 devices and means, and that are transmitted, shared, or accessed through networks.

17
18 20. Defendant derives substantial economic benefits from the Private Information that
19 it collects from Plaintiff and Class Members. For example, Defendant uses and discloses
20 individual’s health information to doctors, nurses, technicians, staff, and other healthcare
21 professionals who become involved in a patient’s care to provide, coordinate or manage a patient’s
22 healthcare; to receive payment for services it has provided or to obtain authorizations for proposed
23 treatments; and to run operations generally.

24
25 21. Defendant knows that “[a]lthough [a patient’s] medical record is the property of
26 Maxim, the information belongs to [the patient].”³ Defendant knew or should have known that by

27
28 ² <https://www.maximhealthcare.com/about-maxim-healthcare/> (last visited Nov. 15, 2022).

³ <https://www.maximhealthcare.com/privacy-security-center/privacy-policy/> (last visited Nov. 15, 2022).

1 collecting and maintaining Private Information, it assumed obligations created by state law,
2 contract, industry standards, common law, and its own promises and representations made to
3 Plaintiff and Class Members that it would keep their Private Information confidential and protect
4 it from unauthorized access and disclosure.

5 **B. Maxim’s Privacy Statements And Representations**

6 22. Defendant holds itself out as respecting individuals’ privacy to gain the trust of its
7 patients and the individuals who use its products and services.

8 23. Defendant made express and implied representations concerning its commitment
9 to user privacy, data security, and regulatory compliance that would lead a reasonable person in
10 similar circumstances to believe that Defendant had, has, and will maintain in place reasonable
11 cybersecurity practices and procedures to protect from unlawful use or disclosure any Private
12 Information it collects or maintains in the regular course of business.
13

14 24. For example, Maxim’s Privacy Policy⁴ provides, in part:

15 The Maxim Healthcare Services family of companies (collectively referred
16 to as “Maxim”) respect your right to privacy. Maxim has created this
17 privacy statement (“Privacy Statement”) to demonstrate our firm
18 commitment to your right to privacy. This Privacy Statement outlines our
personal data handling practices for this Web site.

19 25. Additionally, Maxim’s Patient Privacy Practices⁵ notice states, in part:

20 Maxim Healthcare Services (“Maxim”) *is required by law to secure and*
21 *safeguard your protected health information (“PHI”).* We are further
22 required to provide you with this Notice explaining the Company’s privacy
23 practices with regard to your PHI. This Notice tells you how we may use
24 and disclose your PHI and it outlines those instances where your PHI may
be released without your authorization. You have certain rights regarding
the privacy of your PHI and we also describe those rights in this notice.

25 As used in this notice, Protected Health Information (“PHI”) includes both
26 medical information regarding your care and treatment and individually

27 ⁴ <https://www.maximhealthcare.com/privacy-policy/> (last visited Nov. 15, 2022).

28 ⁵ <https://www.maximhealthcare.com/privacy-security-center/privacy-policy/> (emphasis added) (last visited Nov. 15, 2022).

1 identifiable personal information such as your name, address, phone
2 number, social security number or other personal information that you
3 provide in the course of your treatment. This information may be in
4 electronic, written and/or oral form.

5 **USES OR DISCLOSURES OF PHI.** *Maxim may not use or disclose your*
6 *PHI without your permission* and, once your permission has been obtained,
7 we must use or disclose your PHI only as provided for in the specific terms
8 of that permission.

9

10 **BREACH NOTIFICATION REQUIREMENTS:** Maxim is required to
11 notify you if *unsecured PHI is acquired, accessed, used and/or disclosed*
12 *by an unauthorized party*. Under the Federal Rules, notification must occur
13 without unreasonable delay and in no case later than 60 days of the event.
14 Some State regulations require shorter notification periods and Maxim
15 shall comply with all such requirements.

16 26. Defendant broke these promises to Plaintiff and Class Members when, e.g., as
17 further discussed below, it failed to implement basic industry-standard cybersecurity measures
18 like using multifactor authentication methods to grant access to employee email accounts.

19 27. Plaintiff and Class Members value the privacy and confidentiality of their Private
20 Information and have taken reasonable steps to protect and maintain the confidentiality of their
21 Private Information, including being very careful about sharing their Private Information and
22 destroying or storing any documents containing their Private Information in a safe and secure
23 location.

24 28. Plaintiff and Class Members disclosed their Private Information to Defendant in
25 an environment of privacy and confidentiality entailing fiduciary obligations of confidentiality.

26 29. Plaintiff and Class Members revealed their Private Information to Defendant with
27 the understanding, whether express or implicit, that Defendant would keep the information
28 confidential and secure and would not share or disclose it without the data subject's consent in
the absence of legitimate business reasons for doing so.

1 30. Plaintiff and Class Members relied on Defendant’s superior knowledge, skill, and
2 sophistication to safeguard the confidentiality and integrity of their Private Information
3 confidential.

4 31. No reasonable person, including Plaintiff, would have provided their Private
5 Information without an understanding that Defendant would take reasonable steps to protect that
6 information consistent with its promises, its legal obligations, and the implied terms of its express
7 contracts.

8
9 **C. The Data Breach**

10 32. On or about December 4, 2020, Defendant discovered that an unauthorized
11 malicious actor breached the security of its information system and of the information the system
12 processes, stores, and transmits by gaining access to Maxim’s employees’ email accounts.

13 33. During Defendant’s investigation of the breach, it learned that the malicious actor
14 had unauthorized access to the email accounts for 64 days, between October 1, 2020 and
15 December 4, 2020, before the intrusion was detected.

16 34. After performing a review of the contents of the compromised email accounts,
17 Defendant further discovered that the malicious actor had access to emails and attachments
18 containing Plaintiff and Class Members’ Private Information, including names, addresses, dates
19 of birth, contact information, medical history, medical condition or treatment information,
20 medical record number, diagnosis code, patient account number, Medicare/Medicaid number,
21 username/password, and Social Security numbers (“SSNs”).
22

23 35. California law requires businesses to notify any California resident whose
24 unencrypted personal information was acquired, or reasonably believed to have been acquired, by
25 an unauthorized person. California law also requires that a sample copy of a breach notice sent to
26
27
28

1 more than 500 California residents must be provided to the California Attorney General. Cal. Civ.
2 Code § 1798.82.

3 36. Based upon Defendant's form letter submitted to the Attorney General of the State
4 of California and mailed to Plaintiff and the Class attached hereto as Exhibit A, Defendant was
5 aware that Plaintiff's and the Class's unencrypted personal information was, or was reasonably
6 believed to have been, acquired by an unauthorized person no later than December 4, 2020, but
7 did not notify regulatory authorities or begin to mail notification letters to Plaintiff and the Class
8 until November 4, 2021. In other words, Defendant waited at least 335 days *before beginning to*
9 *mail notification letters* to Plaintiff and the Class of the Data Breach and notifying the regulatory
10 authorities.

11
12 37. Defendant's decision to wait 335 days before beginning to notify Plaintiff and the
13 Class, therefore, was not because a law enforcement agency advised Defendant that the
14 notification would impede a criminal investigation.

15
16 38. Additionally, Plaintiff believes and alleges that there were no measures taken by
17 Defendant to determine the scope of the breach or to restore the reasonable integrity of their
18 computer systems, which justify Defendant's decision to wait 335 days before beginning to issue
19 the notification required by Cal. Civ. Code § 1798.82.

20
21 39. Moreover, Defendant's notifications, including the letters mailed to Plaintiff and
22 the Class, failed to state whether notification was delayed as a result of a law enforcement
23 investigation, in violation of Cal. Civ. Code § 798.82(d)(2)(D).

24
25 40. During the 335-day delay, Plaintiff and Class Members were unaware that their
26 Private Information had been compromised, and that they were, and continue to be, at significant
27 risk of identity theft and various other forms of personal, social, and financial harm.
28

1 41. Implicit in Defendant’s fulfillment of its obligations under Cal. Civ. Code §
2 1798.82, is an acknowledgment that elements of Plaintiff’s and the Class Members’ Private
3 Information were kept in unencrypted form.

4 42. Alternatively, implicit in Defendant’s fulfillment of its obligations under Cal. Civ.
5 Code § 1798.82, is an acknowledgment that its cybersecurity practices were so deficient that the
6 malicious actor was able to gain unauthorized access to an encryption key or credentials and was
7 able to and likely did actually view Plaintiff’s and the Class’s electronic medical information
8 contained in Defendant’s computer systems.

9 43. In its notice of the Data Breach, Defendant further acknowledged that “as an
10 immediate response” to the incident, it was compelled to implement additional security protocols
11 like implementing “Multi-Factor Authentication for all email accounts” and “transition[ing] to a
12 new Security Operations Center with advanced detection and response capabilities.”

13 44. The fact that Defendant was compelled to implement such basic and industry-
14 standard measures in response to the Data Breach cast serious doubt on the reasonableness and
15 adequacy of Defendant’s intrusion prevention and detection procedures and its system-monitoring
16 controls.

17 45. Defendant also represented that it was committed to integrating additional
18 cybersecurity infrastructure and security measures to further harden its digital environment in an
19 effort to prevent a similar event from occurring in the future but has not disclosed what those
20 security measures consist of.

21 46. The compromised information is sensitive enough to materially increase Plaintiff’s
22 and Class Members’ risk of injury, as demonstrated by Defendant’s recommendation that Plaintiff
23 and Class Members spend significant time and take significant actions and precautions to protect
24 themselves from identity fraud and theft, including “remain[ing] vigilant against incidents of
25
26
27
28

1 identity theft and fraud, to review account statements, explanation of benefits, and to monitor
2 credit reports for suspicious activity and to detect errors,” obtaining copies of annual credit
3 reports, placing fraud alerts on credit reports, and placing a security freeze on credit files.

4 47. Plaintiff and Class Members retain a significant interest in ensuring that their
5 Private Information, which remains in Defendant’s possession, is protected from further exposure.

6 48. Backups of the compromised information may remain in Defendant’s possession
7 and is subject to further unauthorized disclosures so long as Defendant fails to undertake
8 appropriate and adequate measures to protect the Private Information.
9

10 49. On information and belief, Defendant has still not implemented critical
11 information systems and data security practices to ensure that affected individuals’ Private
12 Information will not be accessed or stolen by other cyberattackers in the future because, among
13 other things, Defendant focused its response and remediation measures on putting an immediate
14 stop to the present Data Breach.
15

16 **D. Plaintiff Michael Wilson’s Experience**

17 50. Plaintiff Michael Wilson suffers from autism, severe epilepsy, and other medical
18 conditions and has received in-home medical care from Defendant since approximately 2015.

19 51. Throughout his ongoing relationship and course of dealings with Defendant,
20 Plaintiff Wilson provided Private Information to Maxim.

21 52. Plaintiff Michael Wilson’s father and legal conservator, Mosanthony Wilson, was
22 required to provide his son’s Private Information to Defendant in connection with his son’s
23 medical care (including Social Security number, name, date of birth, demographic information,
24 treatment information, provider information, medical record number, and patient account
25 number), as well as some of his own PII (name, address, email address, date of birth, and Social
26 Security number).
27
28

1 53. On or about November 4, 2021, Plaintiff received notice from Defendant that
2 Plaintiff Michael Wilson’s Private Information had been improperly accessed and/or obtained by
3 unauthorized third parties. This notice indicated that, as a result of the data breach, Plaintiff’s
4 Private Information was compromised, which included first name and last name, address, date of
5 birth, demographic information, treatment information, provider information, medical record
6 number, and patient account number.

7 54. Knowing that thieves stole Plaintiff’s Private Information, and knowing that this
8 information may now, or in the future, be available for sale on the dark web has caused Plaintiff
9 anxiety. Plaintiff is now very concerned about how this will impact his healthcare coverage, his
10 medical identity, and about identity theft and fraud in general. This Data Breach has given Plaintiff
11 hesitation about using electronic services and reservations about conducting other online activities
12 requiring Private Information.

13 55. Plaintiff suffered actual injury and damages from having his PII, exposed as a
14 result of the Data Breach including, but not limited to: a) loss of confidentiality; (b) damage to
15 and diminution in the value of Michael Wilson’s PII, a form of property that Defendant obtained
16 from Plaintiff; (c) violation of Michael Wilson’s privacy rights; (d) present, imminent and
17 impending injury arising from the increased risk of medical identity theft and fraud, and; (e) the
18 misuse and/or disclosure of medical information regarding Plaintiff.

19 56. Plaintiff has a continuing interest in ensuring that his Private Information is
20 protected and safeguarded from future breaches.

21 57. Plaintiff has suffered substantial, irreparable harm because his Private Information
22 was compromised, accessed, disclosed, and misused by one or more criminals whose identity
23 remains unknown. Plaintiff must now deal with the overhanging and constant fear and anxiety of
24
25
26
27
28

1 further unauthorized misuse and exploitation of their confidential Private Information for identity
2 theft and fraud and with the humiliation caused by his status as a victim of identity theft or fraud.

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

5 59. As a result of Defendant's wrongful conduct, Plaintiff has spent and will spend
6 significant time and money closely monitoring his identity and credit.

7 60. As a result of Defendant's wrongful conduct, Plaintiff has been required to act in
8 the protection of his interests by bringing this action against Defendant and are entitled to recover
9 reasonable compensation for loss of time, attorney fees, and other expenditures thereby suffered
10 or incurred.

11
12 **E. The Risk, Likelihood, And Magnitude Of Injury Arising From Defendant's**
13 **Information-Security Failures Was Foreseeable And Unreasonable.**

14 ***1. Defendant Knew The Private Information It Stores And Collects Is Highly Valuable***
15 ***And A Target For Identity Thieves.***

16 61. Defendant knew or should have known that the health care industry faces an
17 increased risk of a cybersecurity incident, whether intentional or negligent, that puts Private
18 Information at risk of unauthorized access and disclosure and that the individuals to whom the
19 information concerns are at an increased risk of becoming victims of criminal conduct such as
20 identity theft and fraud, including medical and tax fraud.

21 62. Defendant knew or should have known that by collecting and storing Class
22 Members' Private Information, it undertook a responsibility to take reasonable security measures
23 to protect the information from unlawful use, access, transfer, or disclosure by unauthorized
24 persons.
25
26
27
28

1 63. Private Information is an extremely valuable property right and commodity.⁶ Its
2 value to businesses and identity thieves is axiomatic in today’s “big data” marketplaces.

3 64. The main reason criminals target and steal Private Information is to monetize it by
4 selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort
5 and harass victims and take over victims’ identities to engage in illegal financial transactions
6 under the victims’ names.

7 65. In 2007, the United States Government Accountability Office released a report on
8 data breaches (“GAO Report”) where it explained that “[t]he term ‘identity theft’ is broad and
9 encompasses many types of criminal activities, including fraud on existing accounts—such as
10 unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such
11 as using stolen data to open a credit card account in someone else’s name.”⁷

12 66. Because a person’s identity is akin to a puzzle, the more authentic pieces of data
13 an identity thief obtains about a person, the easier it is for the thief to obtain more information
14 about a victim’s identity, such as a person’s login credentials or Social Security number, and the
15 easier it is to take on the victim’s identity or otherwise harass, track, or defraud the victim. That
16 is, non-PII can easily become PII when combined with additional information gathered from other
17 sources. Once stolen, fraudulent use of that information and damage to victims may continue for
18 years.⁸
19
20
21
22

23 ⁶ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information*
24 (*“PII” Equals the “Value” of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII, which companies
25 obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional
26 financial assets.”) (citations omitted). Available at: <https://scholarship.richmond.edu/jolt/vol15/iss4/2> (last visited
27 Nov. 15, 2022).

28 ⁷ See U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but*
Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007),
<https://www.gao.gov/new.items/d07737.pdf> (last visited Nov. 15, 2022).

⁸ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),
<https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Nov.
15, 2022).

1 67. Medical information is especially valuable to identity thieves. While credit card
2 information and associated PII can sell for as little as \$1-\$2 on the black market, PHI can sell for
3 as much as \$363, according to the Infosec Institute. “Medical identities are 20 to 50 times more
4 valuable to criminals than financial identities. That may explain why approximately 1.5 healthcare
5 data breaches occur each week on average.”⁹

6 68. This is because an individual’s health history (e.g., ailments, diagnosis, surgeries,
7 etc.) cannot be changed.¹⁰ PHI is particularly valuable because criminals can use it to target
8 victims with frauds and scams taking advantage of the victim’s medical conditions. It can be used
9 to create fake insurance claims, allowing for the purchase and resale of medical equipment, or to
10 gain access to prescriptions for illegal use or resale. “A thief may use your name or health
11 insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider,
12 or get other care. If the thief’s health information is mixed with yours, your treatment, insurance
13 and payment records, and credit report may be affected,” putting patients at risk of physical
14 harm.¹¹

15
16
17 69. Therefore, the Private Information targeted, compromised, accessed, and stolen in
18 the Data Breach is significantly more valuable than the loss of, for example, credit card
19 information in a retailer data breach. Unlike credit and debit card accounts, the information
20 compromised in this Data Breach is impossible to “close” and it is difficult, if not impossible, to
21 change one’s Social Security number.

22
23 70. This type of information, therefore, demands a much higher price on the black
24 market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to
25

26 ⁹ <https://www.identityforce.com/personal/medical-identity-theft> (last visited Nov. 15, 2022).

27 ¹⁰ Center for Internet Security, *Data Breaches: In the Healthcare Sector*, available at:
<https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/> (last visited Nov. 15, 2022).

28 ¹¹ See Federal Trade Commission, *What to Know About Medical Identity Theft*,
<http://www.consumer.ftc.gov/articles/0171-medical-identity-theft> (last visited Nov. 15, 2022).

1 credit card information, personally identifiable information and Social Security numbers are
2 worth more than 10x on the black market.”

3 **2. *The Risk Of Injury Was Readily Foreseeable Because The Healthcare Sector Is Faces***
4 ***A Higher Threat Of Targeted Cyberattacks To Obtain Private Information.***

5 71. It is a matter of common knowledge in Defendant’s industry that businesses like
6 Maxim face a higher threat of security breaches due in part to the large amounts of data and Private
7 Information they possess.

8 72. Experts studying cybersecurity routinely identify health care businesses like
9 Defendant’s as particularly vulnerable to cyberattacks because they sit on a gold mine of value
10 Private Information, they often have lesser IT defenses and a high incentive to quickly regain
11 access to their data.

12 73. Additionally, as companies became more dependent on computer systems to run
13 their business, e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of
14 Things (“IoT”), the danger posed by cybercriminals was magnified, thereby highlighting the need
15 for adequate administrative, physical, and technical safeguards.

16 74. In fact, Defendant has an entire page on its website dedicated to consumer fraud
17 alerts where it states that “In recent years, our organization has seen an increase in reports of
18 *phishing attacks* and *identity theft scams* where fraudsters are impersonating Maxim and its
19 representatives in order to gain access to personal information and accounts of their targets.”¹²

20 75. The healthcare sector reported the second largest number of data breaches among
21 all measured sectors in 2018, with the highest rate of exposure per breach.¹³ Indeed, when
22 compromised, healthcare-related data is among the most sensitive and personally consequential.
23
24
25

26 _____
27 ¹² <https://www.maximhealthcare.com/privacy-security-center/consumer-fraud-alerts/> (emphasis added) (last
visited Nov. 15, 2022).

28 ¹³ Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, available at:
<https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/> (last accessed Nov. 15 , 2022).

1 A report focusing on healthcare breaches found the “average total cost to resolve an identity theft-
2 related incident . . . came to about \$20,000,” and that victims were often forced to pay
3 out-of-pocket costs for healthcare they did not receive in order to restore coverage.¹⁴ Almost
4 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly
5 30 percent said their insurance premiums went up after the event. Forty percent of the customers
6 were never able to resolve their identity theft at all. Data breaches and identity theft have a
7 crippling effect on individuals and a detrimental impact on the economy as a whole.¹⁵

8
9 76. Healthcare related data breaches continue to rapidly increase. According to the
10 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security
11 leaders reported having a significant security incident within the previous 12 months, and most of
12 these *known* incidents being caused by “bad actors,” such as cybercriminals.¹⁶ “Hospitals have
13 emerged as a primary target because they sit on a gold mine of sensitive personally identifiable
14 information for thousands of patients at any given time. From social security and insurance
15 policies, to next of kin and credit cards, no other organization, including credit bureaus, have so
16 much monetizable information stored in their data centers.”¹⁷

17
18 77. As a healthcare provider, Defendant knew, or should have known, the importance
19 of safeguarding Private Information entrusted to it by Plaintiff and Class members, and of the
20 foreseeable consequences if its data security systems were breached. This includes the significant
21 costs imposed on Plaintiff and Class members as a result of a breach. Defendant failed, however,
22 to take adequate cybersecurity measures to prevent the Data Breach.

23
24 _____
25 ¹⁴ Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), available at:
<https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed Nov. 15, 2022).

26 ¹⁵ *Id.*

27 ¹⁶ 2019 HIMSS Cybersecurity Survey, available at:
https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last
28 visited Nov. 15, 2022).

¹⁷ Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, available at:
<https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last accessed
Nov. 15, 2022).

1 78. Despite the prevalence of public announcements of data breaches and data security
2 compromises, Defendant failed to take appropriate steps to protect the Private Information of
3 Plaintiff and Class Members from being compromised.

4 79. At all relevant times, Defendant knew or should have known the unique value of
5 the information in its possession, the importance of safeguarding Plaintiff’s and Class Members’
6 Private Information, and the foreseeable injuries that would occur if the security of Defendant’s
7 information system was breached, including the significant economic and noneconomic harms
8 that victims of a data breach would suffer.

9
10 80. Defendant knew or should have known that unencrypted sensitive Private
11 Information amassed in computer systems lacking reasonably adequate cybersecurity measures,
12 such as Defendant’s, is valuable and highly sought after by nefarious third parties seeking to
13 unlawfully monetize that information and commit identity theft and fraud.

14 81. A business using ordinary care would have foreseen that the breach of security, or
15 some similar event, might reasonably result from the tortious conduct described above, and would
16 have taken reasonable precautions against the event.

17
18 **F. Defendant Failed To Implement Reasonable Cybersecurity Measures To Safeguard**
19 **The Private Information Against The Foreseeable Risk Of A Cyberattack And In**
20 **Violation Of Its Statutory Duties.**

21 82. While cybersecurity risks cannot be eliminated entirely, they can be reasonably
22 identified, prevented, and contained through cybersecurity standards, guidelines, and best
23 practices.

24 83. At all relevant times, Defendant knew that it was “required by law to secure and
25 safeguard your protected health information (“PHI”).”¹⁸

26
27
28 ¹⁸ <https://www.maximhealthcare.com/patient-privacy-practices/> (emphasis added) (last visited Nov. 15, 2022).

1 **1. Defendant Failed To Comply With Healthcare Industry Standards.**

2 84. HHS's Office for Civil Rights ("HHS Civil Rights") notes:

3 While all organizations need to implement policies, procedures, and
4 technical solutions to make it harder for hackers to gain access to their
5 systems and data, this is especially important in the healthcare industry.
6 Hackers are actively targeting healthcare organizations, as they store large
7 quantities of highly sensitive and valuable data.¹⁹

8 85. HHS Civil Rights highlights several basic cybersecurity safeguards that can be
9 implemented to improve cyber resilience and require a relatively small financial investment yet
10 can have a major impact on an organization's cybersecurity posture including: (a) the proper
11 encryption of PII and PHI; (b) educating and training healthcare employees on how to protect PII
12 and PHI; and (c) correcting the configuration of software and network devices.

13 86. Private cybersecurity firms have also identified the healthcare sector as being
14 particularly vulnerable to cyberattacks, both because of the value of the PII and PHI they maintain
15 and because as an industry they have been slow to adapt and respond to cybersecurity threats.²⁰
16 These private cybersecurity firms have also promulgated similar best practices for bolstering
17 cybersecurity and protecting against the unauthorized disclosure of PII and PHI.

18 87. Lastly, the Computer Security Division of the National Institute of Standards and
19 Technology's (NIST) Information Technology Laboratory provides standards and technology to
20 protect information systems against threats to the confidentiality, integrity, and availability of
21 information and services.

22 88. Despite the abundance and availability of information regarding the threats and
23 cybersecurity best practices for the healthcare industry to defend against those threats, Defendant
24

25
26

¹⁹ HIPAA Journal, *Cybersecurity Best Practices for Healthcare Organizations*,
27 <https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/> (last visited
28 Nov. 15, 2022).

²⁰ See e.g., INFOSEC, *10 Best Practices For Healthcare Security*, available at:
<https://resources.infosecinstitute.com/topic/10-best-practices-healthcare-security/> (last visited Nov. 15, 2022).

1 chose to ignore them. These best practices were known or should have been known by Defendant,
2 whose failure to heed and properly implement industry standards directly led to the Data Breach
3 and the unlawful exposure of Private Information.

4 89. Defendant knew or should have known its security systems were inadequate,
5 particularly in light of the prior data breaches experienced by similar companies, and yet
6 Defendant failed to take reasonable precautions to safeguard Plaintiff's and Class Members'
7 Private Information.

8 90. Defendant knew or should have known that its conduct created an unreasonable
9 foreseeable risk of harm to the victims of a data breach.

10 91. Defendant failed to disclose the material fact that it did not have in place
11 reasonable procedures to protect the sensitive Private Information it collected from unlawful use
12 or disclosure.

13 92. Had Defendant disclosed this material fact, Plaintiff and Class Members would not
14 have entrusted their Private Information to it.

15
16
17 **G. Plaintiff And Class Members Have And Will Continue To Be Harmed As A**
18 **Consequence Of Defendant's Information-Security Failures And Tortious Conduct.**

19 93. Juxtaposed against the ease of adopting adequate and reasonable cybersecurity
20 practices are the immediate, substantial, and long-lasting harms that Plaintiff and Class Members
21 will suffer due to Defendant's conduct.

22 94. As a direct and proximate result of Defendant's conduct, Plaintiff and Class
23 Members have been placed at an imminent, immediate, and continuing increased risk of harm
24 from fraud and identity theft.

25 95. When individuals have their Private Information stolen, they are at risk for identity
26 theft, and need to: (i) buy identity protection, monitoring, and recovery services; (ii) flag asset,
27 credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers
28

1 to financial institutions, credit agencies, and the Internal Revenue Service; (iii) purchase or
2 otherwise obtain credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and
3 other account statements on a monthly basis for unrecognized credit inquiries, Social Security
4 numbers, home addresses, charges, and/or medical services; (v) place and renew credit fraud alerts
5 on a quarterly basis; (vi) routinely monitor public records, loan data, or criminal records; (vii)
6 contest fraudulent charges and other forms of criminal, financial and medical identity theft, and
7 repair damage to credit and other financial accounts; and (viii) take other steps to protect
8 themselves and recover from identity theft and fraud.
9

10 96. Data breach victims must spend significant time indefinitely monitoring their
11 financial and medical accounts because, generally, there is a significant gap between the time the
12 initial data breach occurs and when it is discovered, and also between the time when Private
13 Information and financial information are stolen and when it is eventually used.

14 97. Private Information is such a valuable commodity to identity thieves that criminals
15 often trade the information on the “cyber black-market” for years once the information has been
16 compromised.
17

18 98. According to the U.S. Government Accountability Office, which conducted a
19 study regarding data breaches:

20 [L]aw enforcement officials told us that in some cases, stolen data might
21 be held for up to a year or more before being used to commit identity theft.
22 Further, once stolen data have been sold or posted on the Web, fraudulent
23 use of that information may continue for years. As a result, studies that
24 attempt to measure the harm resulting from data breaches cannot
25 necessarily rule out all future harm.

26 *See* GAO Report, at p. 29.

27 99. The GAO observed that victims of identity theft will face substantial costs and
28 time to repair the damage to their good name and credit record.

1 100. The FTC recommends that identity theft victims take several steps to protect their
2 personal and financial information after a data breach, including contacting one of the credit
3 bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone
4 steals their identity), reviewing their credit reports, contacting companies to remove fraudulent
5 charges from their accounts, placing a credit freeze on their credit, and correcting their credit
6 reports.²¹

7
8 101. There is a strong probability that entire batches of stolen information have been
9 dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and
10 Class Members are at an increased risk of fraud and identity theft for many years into the future.

11 102. Thus, Plaintiff and Class Members must vigilantly monitor their financial and
12 medical accounts for many years to come.

13 103. Therefore, the fraud and identity monitoring service offered by Defendant is
14 wholly inadequate as the benefits are only provided for 12 months, and it places the burden
15 squarely on Plaintiff and Class Members by requiring them to expend time signing up for that
16 service, as opposed to automatically enrolling all victims of this cybercrime.

17
18 104. As one commentator explained, “[w]hile helpful in detecting identity theft
19 attempts following the breach, credit monitoring is far from a complete solution for several
20 reasons. These reasons include the fact that credit monitoring has limited ability, detecting only
21 credit fraud, and not detecting other types of fraud such as filing a false tax return. Also, credit
22 monitoring is offered for a limited time. Fraudulent use of the stolen credit information often
23 occurs after the credit monitoring ends.”

24
25
26
27
28 _____
²¹ See *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/Steps> (last visited Nov. 15, 2022).

CLASS ACTION ALLEGATIONS

1
2 105. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully
3 set forth herein and further alleges:

4 106. Plaintiff brings this action as a class action on behalf of himself and all other
5 persons similarly situated pursuant to California Code of Civil Procedure section § 382.

6 107. The proposed class which Plaintiff seeks to represent is defined as follows:

7
8 All persons residing in the State of California whose Private Information
9 was compromised, accessed, or viewed in the data breach first announced
 by Maxim on or about November 4, 2021 (the “Class”).

10 108. Excluded from the Class are: (1) Defendant and its affiliates, subsidiaries, officers,
11 directors, legal representatives, and any entity in which Defendant has a controlling interest; (2)
12 members of the judiciary and their staff to whom this action is assigned; (3) individuals who make
13 a timely election to be excluded from this proceeding using the correct protocol for opting out;
14 and (4) Plaintiff's counsel.

15 109. Plaintiff reserves the right to amend the class and definitions if discovery and
16 further investigation reveal that the class should be expanded, narrowed, or otherwise modified.

17
18 110. Certification of Plaintiff’s claims for class-wide treatment is appropriate because
19 Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as
20 would be used to prove those elements in individual actions alleging the same claims for each
21 Class Member.

22 111. This action satisfies the requirements for a class action under California Code of
23 Civil Procedure section § 382, including requirements of numerosity, commonality, typicality,
24 and adequacy of representation, because there is a well-defined community of interest among the
25 persons who comprise the readily ascertainable class defined below and because the Plaintiff is
26 unaware of any difficulties likely to be encountered in managing this case as a class action.
27
28

1 112. **Numerosity:** The Class Members are so numerous that joinder of all members is
2 impracticable. Though the exact number and identities of Class Members are unknown at this
3 time, reports indicate that at least 65,267 had their Private Information compromised in the Data
4 Breach. The identities of Class Members are ascertainable through Defendant’s records, Class
5 Members’ records, publication notice, self-identification, and other means.

6 113. **Commonality.** There are questions of law and fact common to the Class, which
7 predominate over any questions affecting only individual Class Members. These common
8 questions of law and fact include, without limitation:
9

- 10 a. Whether and to what extent Defendant had a duty to protect the Private
11 Information of Plaintiff and Class Members;
- 12 b. Whether Defendant implemented and maintained reasonable security
13 procedures and practices appropriate to the nature and scope of the information
14 maintained by Defendant;
- 15 c. Whether Defendant enabled an unauthorized disclosure of Class Members’
16 Private Information;
- 17 d. Whether there was an unauthorized disclosure by Defendant of Class
18 Members’ Private Information;
- 19 e. Whether Defendant unlawfully used, maintained, lost, or disclosed Class
20 Members’ Private Information;
- 21 f. Whether Defendant misrepresented the safety and security of Class Members’
22 Private Information maintained by Maxim;
- 23 g. Whether Defendant’s data security systems prior to and during the Data Breach
24 complied with applicable data security laws and regulations;
25
26
27
28

- 1 h. Whether Defendant's data security systems prior to and during the Data Breach
2 were consistent with industry standards;
- 3 i. Whether Defendant knew or should have known that its data security systems
4 and monitoring processes were deficient;
- 5 j. Whether and when Defendant became aware of an unauthorized disclosure of
6 Class Members' Private Information;
- 7 k. Whether Defendant violated the law by failing to promptly notify Plaintiff and
8 Class Members that their PHI had been compromised;
- 9 l. Whether Defendant unreasonably delayed notifying Class Members of an
10 unauthorized disclosure of Class Members' Private Information;
- 11 m. Whether Defendant intentionally delayed notifying Class Members of an
12 unauthorized disclosure of Class Members' Private Information;
- 13 n. Whether Defendant's conduct was negligent;
- 14 o. Whether Defendant engaged in unfair, unlawful, or deceptive practices by
15 failing to safeguard the PHI of Plaintiff and Class Members;
- 16 Whether Defendant was unjustly enriched by failing to properly protect
17 Plaintiff's and Class Member's Private Information;
- 18
19

20 114. **Typicality.** Plaintiff's claim is typical of the claims of all the proposed class
21 members, as they are all similarly affected by Defendant's unlawful conduct and their claims are
22 based on such conduct. Plaintiff's Private Information, like that of every other Class Member,
23 was compromised in the Data Breach. Further, Plaintiff's claims are typical of the claims of all
24 proposed class members because their claims arise from the same or similar underlying facts and
25 are based on the same factual and legal theories.
26
27
28

1 115. This class action is also appropriate for certification because Defendant acted or
2 refused to act on grounds generally applicable to the Class, thereby requiring the Court's
3 imposition of uniform relief to ensure compatible standards of conduct toward the Class Members
4 and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's
5 policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge
6 of these policies hinges on Defendant's conduct with respect to the Class each as a whole, not on
7 facts or law applicable only to Plaintiff.

8
9 116. **Fair and Adequate Representation.** Plaintiff and his counsel will fairly and
10 adequately protect the interests of proposed class members. Plaintiff's interests do not conflict
11 with the interests of the class he seeks to represent. Plaintiff has retained counsel who are
12 competent and experienced in class action litigation and complex cases, including data privacy
13 litigation, and will fairly and adequately represent the interests of the proposed class. Plaintiff and
14 his counsel will prosecute this action vigorously.

15
16 117. **Predominance.** Defendant has engaged in a common course of conduct toward
17 Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the
18 same computer systems and unlawfully accessed in the same way. The common issues arising
19 from Defendant's conduct affecting Class Members set out above predominate over any
20 individualized issues. Adjudication of these common issues in a single action has important and
21 desirable advantages of judicial economy.

22
23 118. **Superiority.** A class action is superior to other available methods for the fair and
24 efficient adjudication of the controversy. Class treatment of common questions of law and fact is
25 superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class
26 Members would likely find that the cost of litigating their individual claims is prohibitively high
27 and would therefore have no effective remedy. The prosecution of separate actions by individual
28

1 Class Members would create a risk of inconsistent or varying adjudications with respect to
2 individual Class Members, which would establish incompatible standards of conduct for
3 Defendant. In contrast, the conduct of this action as a Class action presents far fewer management
4 difficulties, conserves judicial resources and the parties' resources, and protects the rights of each
5 Class member.

6 119. Defendant has acted on grounds that apply generally to the Class as a whole, so
7 that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on
8 a Class-wide basis. Unless a Class-wide injunction is issued, Defendant may continue in its failure
9 to properly secure the Private Information of Class Members, Defendant may continue to refuse
10 to provide proper notification to Class Members regarding the Data Breach, and Defendant may
11 continue to act unlawfully as set forth in this Complaint
12

13 120. **Manageability:** The class action will be easily manageable, as the class members
14 are all in the same position and easily identifiable from Defendant's records. Defendant's uniform
15 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class
16 Members demonstrate that there would be no significant manageability problems with
17 prosecuting this lawsuit as a class action. Class Members have already been preliminarily
18 identified and sent notice of the Data Breach by Defendant. Adequate notice can be given to Class
19 Members directly using the information maintained in Defendant's records.
20

21 **CAUSE OF ACTION**

22 **Count I**

23 **Violation Of The California Confidentiality Of Medical Information Act,**
24 **Cal. Civ. Code § 56, et seq.**

25 **(On Behalf of Plaintiff and All Class Members)**

26 121. Plaintiff realleges and incorporates by reference in this count all paragraphs above
27 as if fully set forth herein and further alleges:
28

1 122. Under the California Confidentiality of Medical Information Act, Civil Code §§
2 56, et seq. (hereinafter referred to as the “CMIA”), “medical information” means “any
3 individually identifiable information, in electronic or physical form, in possession of or derived
4 from a provider of health care, health care service plan, pharmaceutical company, or contractor
5 regarding a patient's medical history, mental or physical condition, or treatment.” Cal. Civ. Code
6 § 56.05

7 123. Additionally, Cal. Civ. Code § 56.05 defines “individually identifiable” as
8 meaning that “the medical information includes or contains any element of personal identifying
9 information sufficient to allow identification of the individual, such as the patient's name, address,
10 electronic mail address, telephone number, or social security number, or other information that,
11 alone or in combination with other publicly available information, reveals the identity of the
12 individual.” Cal. Civ. Code § 56.05.

13 124. Under Cal. Civ. Code § 56.101(a) of the CMIA,

14 (a) Every provider of health care, health care service plan, pharmaceutical
15 company, or contractor who creates, maintains, preserves, stores,
16 abandons, destroys, or disposes of medical information shall do so in a
17 manner that preserves the confidentiality of the information contained
18 therein. Any provider of health care, health care service plan,
19 pharmaceutical company, or contractor who negligently creates, maintains,
20 preserves, stores, abandons, destroys, or disposes of medical information
21 shall be subject to the remedies and penalties provided under subdivisions
22 (b) and (c) of Section 56.36.

23 Cal. Civ. Code § 56.101.

24 125. At all relevant times, Defendant was a health care contractor within the meaning
25 of Civil Code § 56.05(d) because it is a “medical group, independent practice association,
26 pharmaceutical benefits manager, or medical service organization and is not a health care service
27 plan or provider of health care.” In the alternative, Defendant is a health care provider within the
28 meaning of Civil Code § 56.06(b) because it “offers software or hardware to consumers, including

1 a mobile application or other related device that is designed to maintain medical information . . .”
2 and maintains medical information as defined by Civil Code § 56.05.

3 126. Plaintiff and Class Members are Defendant’s patients, as defined in Civil Code §
4 56.05(k).

5 127. Plaintiff and Class Members provided their personal medical information to
6 Defendant.

7 128. At all relevant times, Defendant created, maintained, preserved, stored,
8 abandoned, destroyed, or disposed of medical information in the ordinary course business.

9 129. As a result of the Data Breach, Defendant has misused, disclosed, and/or allowed
10 third parties to access and view Plaintiff’s and Class Members’ personal medical information
11 without their written authorization compliant with the provisions of Civil Code §§ 56, et seq. As
12 a further result of the Data Breach, the confidential nature of the plaintiff’s medical information
13 was breached as a result of Defendant’s negligence. Specifically, Defendant knowingly allowed
14 and affirmatively acted in a manner that actually allowed unauthorized parties to access and view
15 Plaintiff’s and Class Members’ Private Information, which was viewed and used when the
16 unauthorized parties engaged in the above-described fraudulent activity. Defendant’s misuse
17 and/or disclosure of medical information regarding Plaintiff and Class Members constitutes a
18 violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.
19

20 130. As a direct and proximate result of Defendant’s wrongful actions, inaction,
21 omissions, and want of ordinary care, Plaintiff’s and Class Members’ personal medical
22 information was disclosed without written authorization.
23

24 131. By disclosing Plaintiff’s and Class Members’ Private Information without their
25 written authorization, Defendant violated California Civil Code § 56, et seq., and their legal duty
26 to protect the confidentiality of such information.
27

- 1 g) For equitable relief compelling Defendant to utilize appropriate methods and
2 policies with respect to consumer data collection, storage, and safety, and to
3 disclose with specificity the type of Private Information compromised during
4 the Data Breach;
- 5 h) For equitable relief requiring restitution and disgorgement of the revenues
6 wrongfully retained as a result of Defendant's wrongful conduct;
- 7 i) Ordering Defendant to pay for not less than three years of credit monitoring
8 services for Plaintiff and the Class;
- 9 j) For an award of actual damages, compensatory damages, statutory damages,
10 and statutory penalties, in an amount to be determined, as allowable by law;
- 11 k) For an award of punitive damages, as allowable by law;
- 12 l) For an award of attorneys' fees and costs, and any other expense, including
13 expert witness fees;
- 14 m) Pre- and post-judgment interest on any amounts awarded; and
- 15 n) Such other and further relief as this Court may deem just and proper.

16 **DEMAND FOR JURY TRIAL**

17 Plaintiff demands a trial by jury of any and all issues in this action so triable.

18 Dated: November 16, 2022

19 Respectfully submitted,

20 /s/ John J. Nelson

21 John J. Nelson (SBN 317598)

22 **MILBERG COLEMAN BRYSON**

23 **PHILLIPS GROSSMAN, PLLC**

24 401 W Broadway, Suite 1760

25 San Diego, CA 92101

26 Tel.: (858) 209-6941

27 Email: jnelson@milberg.com

28 M. Anderson Berry (SBN 262879)

Gregory Haroutunian (SBN 330263)

CLAYEO C. ARNOLD,

A PROFESSIONAL LAW CORP.

865 Howe Avenue

Sacramento, CA 95825

Telephone: (916) 239-4778

Fax: (916) 924-1829

Email: aberry@justice4you.com

gharoutunian@justice4you.com

Attorneys for Plaintiff and the Proposed Class