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

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

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

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

1. **VIOLATIONS OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT**
2. **NEGLIGENCE**

DEMAND FOR JURY TRIAL

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

I. INTRODUCTION

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

[1] As used in this Complaint, personally identifiable information ("PII") generally refers to information that alone or in conjunction with other information identifies an individual, including an individual's contact information (including postal addresses, email addresses, and phone numbers), Social Security number (SSNs), date of birth, driver's license number or government-issued identification number, financial account numbers. See generally Cal. 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."

2. Plaintiff and members of the class are current and former Maxim patients whose Private Information was accessed by an unauthorized malicious actor because Defendant failed to establish reasonable and adequate security practices to safeguard the confidentiality of the patient information Maxim creates, maintains, preserves, stores, abandons, destroys, or disposes.

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

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

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

6. Defendant disregarded Plaintiff's and Class Members' rights by, among other things, intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' Private Information stored within Defendant's information system were protected and safeguarded against unauthorized access, misuse, and disclosure, failing to take basic industry-standard steps to prevent, identify,

contain a breach of its system's security, failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use, and failing to give timely and adequate notice to Plaintiff and Class Members that their Private Information had been subject to the unauthorized access of an unknown third party.

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

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

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

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

II. PARTIES

A. Plaintiff

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

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

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

B. Defendant

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

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

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

III. JURISDICTION AND VENUE

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

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

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

IV. STATEMENT OF FACTS

A. Defendant's Business Practices

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

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

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

///

[2] https://www.maximhealthcare.com/about-maxim-healthcare/ (last visited Nov. 15, 2022).

21. Defendant knows that "[a]lthough [a patient's] medical record is the property of Maxim, the information belongs to [the patient]."[3] Defendant knew or should have known that by collecting and maintaining Private Information, it assumed obligations created by state law, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members that it would keep their Private Information confidential and protect it from unauthorized access and disclosure.

B. Maxim's Privacy Statements And Representations

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

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

24. For example, Maxim's Privacy Policy[4] provides, in part:

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

25. Additionally, Maxim's Patient Privacy Practices[5] notice states, in part:

> Maxim Healthcare Services ("Maxim") *is required by law to secure and safeguard your protected health information ("PHI")*. We are further required to provide you with this Notice explaining the Company's privacy

[3] https://www.maximhealthcare.com/privacy-security-center/privacy-policy/ (last visited Nov. 15, 2022).
[4] https://www.maximhealthcare.com/privacy-policy/ (last visited Nov. 15, 2022).
[5] https://www.maximhealthcare.com/privacy-security-center/privacy-policy/ (emphasis added) (last visited Nov. 15, 2022).

> practices with regard to your PHI. This Notice tells you how we may use 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.
>
> As used in this notice, Protected Health Information ("PHI") includes both medical information regarding your care and treatment and individually identifiable personal information such as your name, address, phone number, social security number or other personal information that you provide in the course of your treatment. This information may be in electronic, written and/or oral form.
>
> **USES OR DISCLOSURES OF PHI**. *Maxim may not use or disclose your PHI without your permission* and, once your permission has been obtained, we must use or disclose your PHI only as provided for in the specific terms of that permission.
>
> . . . .
>
> **BREACH NOTIFICATION REQUIREMENTS**: Maxim is required to notify you if *unsecured PHI is acquired, accessed, used and/or disclosed by an unauthorized party*. Under the Federal Rules, notification must occur without unreasonable delay and in no case later than 60 days of the event. Some State regulations require shorter notification periods and Maxim shall comply with all such requirements.

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

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

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

///

29. Plaintiff and Class Members revealed their Private Information to Defendant with the understanding, whether express or implicit, that Defendant would keep the information 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.

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

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

C. The Data Breach

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

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

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

35. California law requires businesses to notify any California resident whose unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person. California law also requires that a sample copy of a breach notice sent to more than 500 California residents must be provided to the California Attorney General. Cal. Civ. Code § 1798.82.

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

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

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

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

///

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

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

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

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

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

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

///

46. The compromised information is sensitive enough to materially increase Plaintiff's and Class Members' risk of injury, as demonstrated by Defendant's recommendation that Plaintiff and Class Members spend significant time and take significant actions and precautions to protect themselves from identity fraud and theft, including "remain[ing] vigilant against incidents of identity theft and fraud, to review account statements, explanation of benefits, and to monitor credit reports for suspicious activity and to detect errors," obtaining copies of annual credit reports, placing fraud alerts on credit reports, and placing a security freeze on credit files.

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

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

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

D. <u>Plaintiff Michael Wilson's Experience</u>

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

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

52. Plaintiff Michael Wilson's father and legal conservator, Mosanthony Wilson, was required to provide his son's Private Information to Defendant in connection with his son's

medical care (including Social Security number, name, date of birth, demographic information, treatment information, provider information, medical record number, and patient account number), as well as some of his own PII (name, address, email address, date of birth, and Social Security number).

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

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

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

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

57. Plaintiff has suffered substantial, irreparable harm because his Private Information was compromised, accessed, disclosed, and misused by one or more criminals whose identity remains unknown. Plaintiff must now deal with the overhanging and constant fear and anxiety of further unauthorized misuse and exploitation of their confidential Private Information for identity theft and fraud and with the humiliation caused by his status as a victim of identity theft or fraud.

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

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

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

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

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

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

62. Defendant knew or should have known that by collecting and storing Class Members' Private Information, it undertook a responsibility to take reasonable security measures

to protect the information from unlawful use, access, transfer, or disclosure by unauthorized persons.

63. Private Information is an extremely valuable property right and commodity.[6] Its value to businesses and identity thieves is axiomatic in today's "big data" marketplaces.

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

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

66. Because a person's identity is akin to a puzzle, the more authentic pieces of data an identity thief obtains about a person, the easier it is for the thief to obtain more information about a victim's identity, such as a person's login credentials or Social Security number, and the easier it is to take on the victim's identity or otherwise harass, track, or defraud the victim. That is, non-PII can easily become PII when combined with additional information gathered from other

---

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

[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).

sources. Once stolen, fraudulent use of that information and damage to victims may continue for years.[8]

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

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

///

///

[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).

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

[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).

[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).

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

70. This type of information, therefore, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."

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

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

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

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

74. In fact, Defendant has an entire page on its website dedicated to consumer fraud alerts where it states that "In recent years, our organization has seen an increase in reports of

phishing attacks and *identity theft scams* where fraudsters are impersonating Maxim and its representatives in order to gain access to personal information and accounts of their targets."[12]

75. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[13] Indeed, when compromised, healthcare-related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[14] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and a detrimental impact on the economy as a whole.[15]

76. Healthcare related data breaches continue to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident within the previous 12 months, and most of these *known* incidents being caused by "bad actors," such as cybercriminals.[16] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable

---

[12] https://www.maximhealthcare.com/privacy-security-center/consumer-fraud-alerts/ (emphasis added) (last visited Nov. 15, 2022).

[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).

[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).

[15] *Id.*

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

information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[17]

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

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

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

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

///

[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).

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

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

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

83. At all relevant times, Defendant knew that it was "required by law to secure and safeguard your protected health information ("PHI")."[18]

1. Defendant Failed To Comply With Healthcare Industry Standards.

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

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

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

///

[18] https://www.maximhealthcare.com/patient-privacy-practices/ (emphasis added) (last visited Nov. 15, 2022).

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

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

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

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

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

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

///

[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).

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

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

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

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

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

95. When individuals have their Private Information stolen, they are at risk for identity theft, and need to: (i) buy identity protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service; (iii) purchase or otherwise obtain credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services; (v) place and renew credit fraud alerts on a quarterly basis; (vi) routinely monitor public records, loan data, or criminal records; (vii) contest fraudulent charges and other forms of criminal, financial and medical identity theft, and repair damage to credit and other financial accounts; and (viii) take other steps to protect themselves and recover from identity theft and fraud.

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

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

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

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

See GAO Report, at p. 29.

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

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

[21] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Nov. 15 , 2022).

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

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

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

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

V. CLASS ACTION ALLEGATIONS

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

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

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

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

///

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

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

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

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

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

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

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature and scope of the information maintained by Defendant;

c. Whether Defendant enabled an unauthorized disclosure of Class Members' Private Information;

d. Whether there was an unauthorized disclosure by Defendant of Class Members' Private Information;

e. Whether Defendant unlawfully used, maintained, lost, or disclosed Class Members' Private Information;

f. Whether Defendant misrepresented the safety and security of Class Members' Private Information maintained by Maxim;

g. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

j. Whether and when Defendant became aware of an unauthorized disclosure of Class Members' Private Information;

k. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PHI had been compromised;

l. Whether Defendant unreasonably delayed notifying Class Members of an unauthorized disclosure of Class Members' Private Information;

m. Whether Defendant intentionally delayed notifying Class Members of an unauthorized disclosure of Class Members' Private Information;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI of Plaintiff and Class Members;

Whether Defendant was unjustly enriched by failing to properly protect Plaintiff's and Class Member's Private Information;

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

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

116. **Fair and Adequate Representation**: Plaintiff and his counsel will fairly and adequately protect the interests of proposed class members. Plaintiff's interests do not conflict

with the interests of the class he seeks to represent. Plaintiff has retained counsel who are competent and experienced in class action litigation and complex cases, including data privacy litigation, and will fairly and adequately represent the interests of the proposed class. Plaintiff and his counsel will prosecute this action vigorously.

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

118. **Superiority:** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

119. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse

to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint

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

VI. CAUSE OF ACTION

Count I

Violation Of The California Confidentiality Of Medical Information Act, Cal. Civ. Code § 56, et seq. (On Behalf of Plaintiff and All Class Members)

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

122. Under the California Confidentiality of Medical Information Act, Civil Code §§ 56, et seq. (hereinafter referred to as the "CMIA"), "medical information" means "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." Cal. Civ. Code § 56.05

123. Additionally, Cal. Civ. Code § 56.05 defines "individually identifiable" as meaning that "the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address,

electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual." Cal. Civ. Code § 56.05.

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

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

Cal. Civ. Code § 56.101.

125. At all relevant times, Defendant was a health care contractor within the meaning of Civil Code § 56.05(d) because it is a "medical group, independent practice association, pharmaceutical benefits manager, or medical service organization and is not a health care service plan or provider of health care." In the alternative, Defendant is a health care provider within the meaning of Civil Code § 56.06(b) because it "offers software or hardware to consumers, including a mobile application or other related device that is designed to maintain medical information . . ." and maintains medical information as defined by Civil Code § 56.05.

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

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

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

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

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

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

132. Defendant also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

133. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff's and Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff's and Class Members' written authorization.

///

134. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violation of the CMIA, Plaintiff and Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Plaintiff and Class Member, (iii) punitive damages of up to $3,000 per Plaintiff and Class Member, and (iv) attorneys' fees, litigation expenses and court costs under California Civil Code § 56.35.

Count II

Negligence
(On Behalf of Plaintiff and All Class Members)

135. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 120.

136. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, using, and/or protecting their PII/PHI from unauthorized third parties.

137. The legal duties owed by Defendant to Plaintiff and Class Members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI of Plaintiff and Class Members in its possession;
b. To protect PII/PHI of Plaintiff and Class Members in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and
c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class Members of the Data Breach.

///

138. Defendant breached its duties to Plaintiff and Class Members. Defendant knew or should have known the risks of collecting and storing PII/PHI and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

139. Defendant knew or should have known that its security practices did not adequately safeguard Plaintiff's and Class Members' PII/PHI.

140. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PII/PHI of Plaintiff and those of the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' PII/PHI during the period it was within Defendant's possession and control.

141. Defendant admits that a "number of employees' email accounts were accessed without authorization between October 1, 2020 and December 4, 2020," and "the investigation was not able to determine exactly which email messages or attachments may have been accessed or viewed without authorization."

142. Defendant breached the duties it owed to Plaintiff and Class Members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect PII and thereby creating a foreseeable risk of harm;
b. Failing to comply with the minimum industry data security standards during the period of the Data Breach to detect and prevent a breach;
c. Failing to act despite knowing or having reason to know that its systems were vulnerable to attack; and
d. Failing to timely and accurately disclose to consumers that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

143. Due to Defendant's conduct, Plaintiff and Class Members are entitled to comprehensive identity monitoring and credit monitoring. Identity and credit monitoring is reasonable here because the PII/PHI taken can be used for identity theft and other types of financial fraud against Plaintiff and the Class Members.

144. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

145. As a result of Defendant's negligence, Plaintiff and Class Members suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII/PHI, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI in its continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members, including ongoing credit monitoring.

146. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the Class Members suffered was the direct and proximate result of Defendant's negligent conduct.

///

///

VII. RELIEF REQUESTED

WHEREFORE, Plaintiff, individually and on behalf of the Classes defined herein, pray for judgment against Maxim as follows:

a) Certifying this case as a class action; certifying Plaintiff as class representative and their counsel as class counsel;

b) An award to Plaintiff and the class of all forms of recovery allowed under law and equity including rescission, restitution, disgorgement, injunctive and other equitable relief, and compensatory and punitive damages;

c) An award of attorneys' fees and costs, as allowed by law;

d) An award of pre-judgment and post-judgment interest, as provided by law;

e) For an Order certifying this action as a Class action and appointing Plaintiff and their counsel to represent the Class;

f) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

g) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

h) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

i) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

j) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

k) For an award of punitive damages, as allowable by law;

l) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

m) Pre- and post-judgment interest on any amounts awarded; and

n) Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

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

Dated: December 20, 2022

Respectfully submitted,

CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.

/s/ M. Anderson Berry -
M. Anderson Berry, Esq.

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

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

Attorneys for Plaintiff and the Proposed Class