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]

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."

70. This type of information, therefore, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared 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.

[11] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited May 16, 2022).

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

[12] https://www.maximhealthcare.com/maxim-healthcare-compliance-and-ethics/consumer-fraud-alerts/ (emphasis added) (last visited May 16, 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 May 24, 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 May 24, 2022).
[15] *Id.*

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 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,

[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 May 19, 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 May 24, 2022).

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.

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]

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

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.

---

[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 May 19, 2022).

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 medical 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]

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 medical identity theft for many years into the future.

102. Thus, Plaintiff and Class Members must vigilantly monitor their financial and

[21] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited May 16, 2022).

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, "While 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."

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 violated the California Confidentiality of Medical Information Act ("CMIA");

o. Whether Plaintiff and Class Members are entitled to damages, civil penalties,