KOPELOWITZ OSTROW P.A.
Kristen Lake Cardoso (SBN 338762)
cardoso@kolawyers.com
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100

Counsel for Plaintiffs and the Putative Class

[Additional counsel listed on signature page]

SUPERIOR COURT FOR THE STATE OF CALIFORNIA
COUNTY OF SAN DIEGO

CLARISSA CASTRO, AMBER FRIEDRICH, DUNCAN MEADOWS, JOHN SOUTH, and NYREE ZAPATA, *individually and on behalf of all others similarly situated,* Plaintiffs, v. **ARCH HEALTH PARTNERS, INC. d/b/a PALOMAR HEALTH MEDICAL GROUP,** Defendant.	**Case No. 37-2024-00024339-CU-NP-CTL** **PLAINTIFFS' AMENDED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Clarissa Castro, Amber Friedrich, Duncan Meadows, John South, and Nyree Zapata (together, "Plaintiffs") bring this Amended Class Action Complaint on behalf of themselves, and all others similarly situated, against Defendant, Arch Health Partners, Inc. d/b/a Palomar Health Medical Group ("Palomar Health Medical Group" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to them, which are based on personal knowledge:

NATURE OF THE ACTION

1. This class action arises from Defendant's failure to properly secure, safeguard, and adequately destroy Plaintiffs' and Class Members' sensitive personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") that it had acquired and stored for its business purposes.

2. Defendant's data security failures allowed a targeted cyberattack to compromise

Defendant's network (the "Data Breach") that, upon information and belief, contained Private Information of Plaintiffs and other individuals ("Class Members," defined below). Defendant initially disclosed disruptions in the functioning of its patient portal no later than March 28, 2024, at which time it "anticipate[d] that this issue will be resolved by Friday, March 29, 2024." Defendant became aware that the disruption was due to suspicious activity on or about May 5, 2024. Thereafter, Defendant emailed individuals whose Private Information was held in its system, including Plaintiffs, that it had experienced a cybersecurity incident (the "Notice Email").[1]

3. Defendant is a medical group that owns and operates hospitals, clinics, laboratories, out-patient centers, and nursing facilities across the San Diego, California area.[2]

4. Defendant admits Plaintiffs' and Class Members' Private Information was unlawfully accessed and may have been exfiltrated by an unauthorized actor.

5. The Private Information compromised in the Data Breach included Private Information of Plaintiffs and Class Members that was maintained by Defendant.

6. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted for treatment with Defendant.

7. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure Private Information from those risks left that property in a dangerous condition.

8. Upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiffs and Class

[1] A true and correct copy of the "Notice Email" is attached hereto as ***Exhibit A***.
[2] https://www.palomarhealth.org/.

Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

9. Defendant impliedly understood its obligations and promised to safeguard Plaintiffs' and Class Members' Private Information. Plaintiffs and Class Members relied on these implied promises when seeking out and paying for Defendant's services. But for this mutual understanding, Plaintiffs and Class Members would not have provided Defendant with their Private Information. Defendant, however, did not meet these reasonable expectations, causing Plaintiffs and Class Members to suffer injury.

10. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members with prompt and full notice of the Data Breach.

11. In addition, Defendant failed to properly monitor the computer network and systems that housed the Private Information. Had it properly monitored its property, it would have discovered the intrusion sooner rather than allowing cybercriminals a period of unimpeded access to the Private Information of Plaintiffs and Class Members.

12. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

13. As a result of the Data Breach, Plaintiffs and Class Members are now at a current,

imminent, and ongoing risk of fraud and identity theft. Plaintiffs and Class Members must now and for years into the future closely monitor their medical and financial accounts to guard against identity theft. As a result of Defendant's unreasonable and inadequate data security practices, Plaintiffs and Class Members have suffered numerous actual and concrete injuries and damages.

14. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that the Plaintiffs' and Class Members' Private Information was targeted, accessed, has been misused, and disseminated on the dark web.

15. Plaintiffs and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will continue to include in the future, among other things: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against the imminent risk of identity theft.

16. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (g) deprivation of value of their PII; and (h) the continued risk to their sensitive Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it collected and maintained.

17. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

18. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence and negligence *per se*, (ii) violation of the California Consumer Privacy Act, (iii) violation of the California Confidentiality of Medical

Information Act, (iv) violation of the California Customer Records Act, and (v) invasion of privacy.

19. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

20. The exposure of one's Private Information to cybercriminals is a bell that cannot be un-rung. Before this Data Breach, Plaintiffs' and the Class's Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

PARTIES

21. Plaintiff Castro is an adult individual who at all relevant times has been a citizen and resident of California.

22. Plaintiff Friedrich is an adult individual who at all relevant times has been a citizen and resident of California.

23. Plaintiff Meadows is an adult individual who at all relevant times has been a citizen and resident of California.

24. Plaintiff South is an adult individual who at all relevant times has been a citizen and resident of California.

25. Plaintiff Zapata is an adult individual who at all relevant times has been a citizen and resident of California.

26. Defendant Arch Health Partners, Inc. d/b/a Palomar Health Medical Group is a California corporation with its principal place of business located at 15611 Pomerado Rd, Suite 400 Poway, CA 92064-2437.

JURISDICTION AND VENUE

27. This Court has jurisdiction over this action under Code of Civil Procedure § 410.10 because the total amount of aggregate damages incurred by Plaintiffs and Class Members exceeds $25,000. Further, upon information and belief, the amount in controversy as to Plaintiffs, individually, does not exceed $75,000.

28. This Court has personal jurisdiction over Defendant because it is a California corporation that operates and has its principal place of business in this District and conducts substantial business in this District.

29. This action does not qualify for federal jurisdiction under the Class Action Fairness Act because the home estate controversy exception under 28 U.S.C. § 1332 (d)(4)(B) applies to this action because (1) more than two-thirds of the members of the proposed Class are citizens of California, and (2) Defendant is a citizen of California, given that it is domiciled in California and has it principle place of business in California.

30. Venue is proper in this Court pursuant to Code of Civil Procedure §§ 395(a) and 395.5 and California Bus. & Prof. Code § 17203 because Defendant transacts business in this District and a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is domiciled in this District, maintains Plaintiffs' and Class Members' Private Information in this District, and has caused harm to Plaintiffs and Class Members in this District.

FACTUAL BACKGROUND

A. Defendant Knew the Risks of Storing Valuable Private Information and the Foreseeable Harm to Victims.

31. At all relevant times, Defendant knew it was storing its patient's Private Information on its internal network server and that, as a result, Defendant's systems would be attractive targets for cybercriminals.

32. Defendant also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised, as well as intrusion into their highly private health information.

33. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

34. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime

forums on the dark web that serve as a bustling marketplace for such commerce."[3] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

35. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the ITRC, in 2019, there were 1,473 reported data breaches in the United States, exposing 164 million sensitive records and 705 million "non-sensitive" records.[4]

36. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. For instance, in 2018, 14.4 million people were victims of some form of identity fraud, and 3.3 million people suffered unrecouped losses from identity theft, nearly three times as many as in 2016. And these out-of-pocket losses more than doubled from 2016 to $1.7 billion in 2018.[5]

37. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[6]

38. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[7]

39. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

---

[3] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.
[4] *Data Breach Reports: 2019 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 2, *available at* https://notified.idtheftcenter.org/s/resource#annualReportSection.
[5] Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available at https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(1).
[6] https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/.
[7] *Id.*

40. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[8] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[9]

41. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[10]

42. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can **sell for up to $1,000 online.**"[11]

43. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before

---

[8] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[9] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Key findings from The Global State of Information Security® Survey 2015: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[10] Experian, Healthcare Data Breach: What to Know About them and What to Do After One: https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[11] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] 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."[12]

44. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

B. Defendant Breached its Duty to Protect its Patients' Private Information

45. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, and the Health Insurance Portability and Accountability Act ("HIPAA"). Under state and federal law, businesses like Defendant have duties to protect its current and former patients' PII/PHI and to notify them about breaches.

46. The Private Information held by Defendant in its computer system and network included the highly sensitive Private Information of Plaintiffs and Class Members.

47. On March 28, 2024, certain Class Members received an emailed letter from Defendant reporting that "some outbound secure messages and documents" sent from its patient portal were "not being delivered to patients, despite notifications indicating that they are available." Defendant claimed to "anticipate that this issue will be resolved by Friday, March 29, 2024.

48. On or around May 5, 2024, Defendant detected the suspicious activity on its system. Defendant's investigation revealed that hackers had access to its network from April 23, 2024, to May

[12] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf.

5, 2024.[13] According to Defendant, certain files were exfiltrated from its network, which may be "unrecoverable."[14]

49. On May 21, 2024, certain Class Members received an email from Defendant reporting on the "ongoing cybersecurity incident" on its systems. On or around June 12, 2024, certain Class Members received an email from Palomar to similar effect.

50. As of July 11, 2024, Defendant's website reported that Defendant "continues to work with third-party forensic specialists to restore operations across our network" and "plan[s] to have all systems fully restored to their original state by July 18, 2024."[15]

51. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures, in order to protect its current and former patients' Private Information.

C. Plaintiffs' Experiences

Clarissa Castro

52. Plaintiff Castro (for purposes of this section, "Plaintiff") is a former patient of Defendant. As a patient, she was required to provide her Private Information to Defendant, including among other things, all her contact information, her Social Security number, her medical records number, her health insurance information and other private information.

53. Plaintiff diligently protects her Private Information and has never knowingly sent unencrypted Private Information over the Internet.

54. Plaintiff is not aware of ever being part of a data breach involving her medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, she has taken multiple steps to avoid identity theft, including increasingly reviewing her credit monitoring service, setting up notices and reports, and carefully reviewing all her accounts.

[13] https://www.hipaajournal.com/patient-data-compromised-in-palomar-health-medical-group-cyberattack/.
[14] *Id.*
[15] https://www.palomarhealthmedicalgroup.org/phmg-update/

55. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors her Private Information multiple times a week and has already spent many hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

56. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud. Upon information and belief, as a result of the Data Breach, Plaintiff has experienced increased amounts of spam email, texts and phones calls. Specifically, she has received emails stating her insurance is going to lapse and to send money. She has also received texts regarding medical information from CVS, which CVS confirmed to Plaintiff were not sent by CVS. Further, she has received multiple suspicious text messages asking her to scan barcodes.

57. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

58. Plaintiff greatly values her privacy, and would not have provided her Private Information, undertaken the services and paid the amounts that she did if she had known that her Private Information would be maintained using inadequate data security systems.

Amber Friedrich

59. Plaintiff Friedrich (for purposes of this section, "Plaintiff") has been a patient of Defendant for approximately 20 years. As a patient, she was required to provide her Private Information to Defendant, including among other things, all her contact information, her Social

Security number, her medical records number, her health insurance information and other private information.

60. Plaintiff diligently protects her Private Information and has never knowingly sent unencrypted Private Information over the Internet.

61. Plaintiff is not aware of ever being part of a data breach involving her medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, she has taken multiple steps to avoid identity theft, including increasingly reviewing her credit monitoring service, setting up notices and reports, and carefully reviewing all her accounts.

62. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, checking to confirm that she is on the FCC's Do Not Call List, discussing the Data Breach with her medical providers at Defendant to better understand why they have been unable to retrieve her medical data, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors her Private Information and has spent time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

63. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud. Upon information and belief, as a result of the Data Breach, Plaintiff has experienced increased amounts of spam email, texts and phones calls. Plaintiff also been precluded from receiving copies of her x-rays from her medical providers as a result of the Data Breach.

64. Plaintiff has also experienced increased anxiety as a result of the Data Breach because her medical providers at Defendant have been unable to show her x-rays because of the Data Breach, which she previously relied on to track the progress of her recovery from an injury and to discuss them with her family.

65. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

66. Plaintiff greatly values her privacy, and would not have provided her Private Information, undertaken the services and paid the amounts that she did if she had known that her Private Information would be maintained using inadequate data security systems.

Duncan Meadows

67. Plaintiff Meadows (for purposes of this section, "Plaintiff") is a former patient of Defendant. As a patient, he was required to provide his Private Information to Defendant, including among other things, all his contact information, his Social Security number, his medical records number, his health insurance information and other private information.

68. Plaintiff diligently protects his Private Information and has never knowingly sent unencrypted Private Information over the Internet.

69. Plaintiff is not aware of ever being part of a previous data breach involving his medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, he has taken multiple steps to avoid identity theft, including increasingly reviewing his credit monitoring service, setting up notices and reports, and carefully reviewing all his accounts.

70. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff monitors his Private Information and has already spent many hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

71. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft

and fraud. Upon information and belief, as a result of the Data Breach, Plaintiff has experienced increased amounts of spam email, texts and phones calls. Plaintiff was also recently notified by his credit monitoring services that his Social Security number is on the dark web.

72. Plaintiff has also suffered increased stress and anger as a result of the Data Breach, for which he has undergone counseling.

73. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

74. Plaintiff greatly values his privacy, and would not have provided his Private Information, undertaken the services and paid the amounts that he did if he had known that his Private Information would be maintained using inadequate data security systems.

John South

75. Plaintiff South (for purposes of this section, "Plaintiff") has been a patient of Defendant for approximately 10 years. As a patient, he was required to provide his Private Information to Defendant, including among other things, all his contact information, his Social Security number, his medical records number, his health insurance information and other private information.

76. Plaintiff diligently protects his Private Information and has never knowingly sent unencrypted Private Information over the Internet.

77. Plaintiff is not aware of ever being part of a data breach involving his medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, he has taken multiple steps to avoid identity theft, including increasingly reviewing his credit monitoring service, setting up notices and reports, and carefully reviewing all his accounts.

78. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Not only does Plaintiff spend time monitoring his Private Information, but he has also spent

time visiting Defendant's place of business to schedule appointments with his medical providers and calling Defendant to address an issue regarding one of his prescriptions that arose because Defendant's systems were not working properly as a result of the Data Breach. Thus, Plaintiff has already spent multiple hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

79. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud. Upon information and belief, as a result of the Data Breach, Plaintiff has experienced increased amounts of spam email, texts and phones calls.

80. Also, after the Data Breach, in or around May 2024, Plaintiff discovered an incorrect charge in the amount of $139 from Defendant on his Experian credit report. He engaged Credit Saint to address the issue and other incorrect entries on his credit report. Upon information and belief, this incorrect charge from Defendant was a result of the Data Breach.

81. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

82. Plaintiff greatly values his privacy, and would not have provided his Private Information, undertaken the services and paid the amounts that he did if he had known that his Private Information would be maintained using inadequate data security systems.

Nyree Zapata

83. Plaintiff Zapata (for purposes of this section, "Plaintiff") is a former patient of Defendant. As a patient, she was required to provide her Private Information to Defendant, including among other things, all her contact information, her Social Security number, her medical records number, her health insurance information and other private information.

84. Plaintiff diligently protects her Private Information and has never knowingly sent unencrypted Private Information over the Internet.

85. Plaintiff is not aware of ever being part of a data breach involving her medical records and is concerned that it and other Private Information has now been exposed to bad actors. As a result, she has taken multiple steps to avoid identity theft, including increasingly reviewing her credit monitoring service, setting up notices and reports, and carefully reviewing all her accounts.

86. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, changing passwords, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff has tried calling Defendant regarding the Data Breach, but has been unable to communicate with Defendant because Defendant does not answer telephone calls and instead requires callers to leave a message for a return call. Plaintiff monitors her Private Information multiple times a week and has already spent many hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

87. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud. Upon information and belief, as a result of the Data Breach, Plaintiff has experienced increased amounts of spam email, texts and phones calls. Plaintiff also been precluded from requesting lab results, medical records, or feedback from her medical providers through Defendant's website as a result of the Data Breach.

88. Plaintiff has also experienced increased anxiety and worry as a result of the Data Breach because the cybercriminals who stole her Private Information can use it any time to commit identity theft and fraud.

89. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result

of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

90. Plaintiff greatly values her privacy, and would not have provided her Private Information, undertaken the services and paid the amounts that she did if she had known that her Private Information would be maintained using inadequate data security systems.

D. Plaintiffs and Class Members Suffered Damages

91. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways. Plaintiffs and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

92. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct. Further, the value of Plaintiffs' and Class Members' Private Information has been diminished by its exposure in the Data Breach.

93. As a result of Defendant's failures, Plaintiffs and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of Private Information.

94. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud – this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[16]

[16] https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.

95. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[17]

96. "Actors buying and selling Private Information from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[18]

97. The reality is that cybercriminals seek nefarious outcomes from a data breach" and "stolen health data can be used to carry out a variety of crimes."[19]

98. Health information in particular is likely to be used in detrimental ways – by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[20]

99. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[21]

100. Plaintiffs and Class Members have also been injured by Defendant's unauthorized disclosure of their confidential and private medical records and PHI.

101. Plaintiffs and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its current and former patients' Private Information.

---

[17] https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud.
[18] *Id.*
[19] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[20] *Id.*
[21] https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

COMMON INJURIES AND DAMAGES

102. As result of Defendant's ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

103. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including but not limited to: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their Private Information; and (i) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

A. The Risk of Identity Theft to Plaintiffs and Class Members is Present and Ongoing

104. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

105. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

106. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking

whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

107. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[22] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[23] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

108. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the Private Information at issue here.[24] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[25] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[26]

109. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are

---

[22] *What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[23] *Id.*
[24] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[25] *Id.; What Is the Dark Web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[26] *What is the Dark Web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[27]

110. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

111. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

112. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social

---

[27] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

Security number to apply for additional credit lines.[29]

113. Theft of PHI, in particular, is gravely serious: "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."[30]

114. One such example of criminals using PHI for profit is the development of "Fullz" packages. Cyber-criminals can cross-reference two sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

115. The development of "Fullz" packages means that stolen PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and Class Members' stolen PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

116. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[31]

117. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[32] Defendant did not rapidly report

[29] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.
[30] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.
[31] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.
[32] *Id.*

to Plaintiffs and the Class that their Private Information had been stolen.

118. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

119. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

120. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PHI. To protect themselves, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

121. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[33]

122. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy

[33] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[34]

123. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[35]

124. Defendant's failure to notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

B. Loss of Time to Mitigate the Risk of Identify Theft and Fraud

125. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

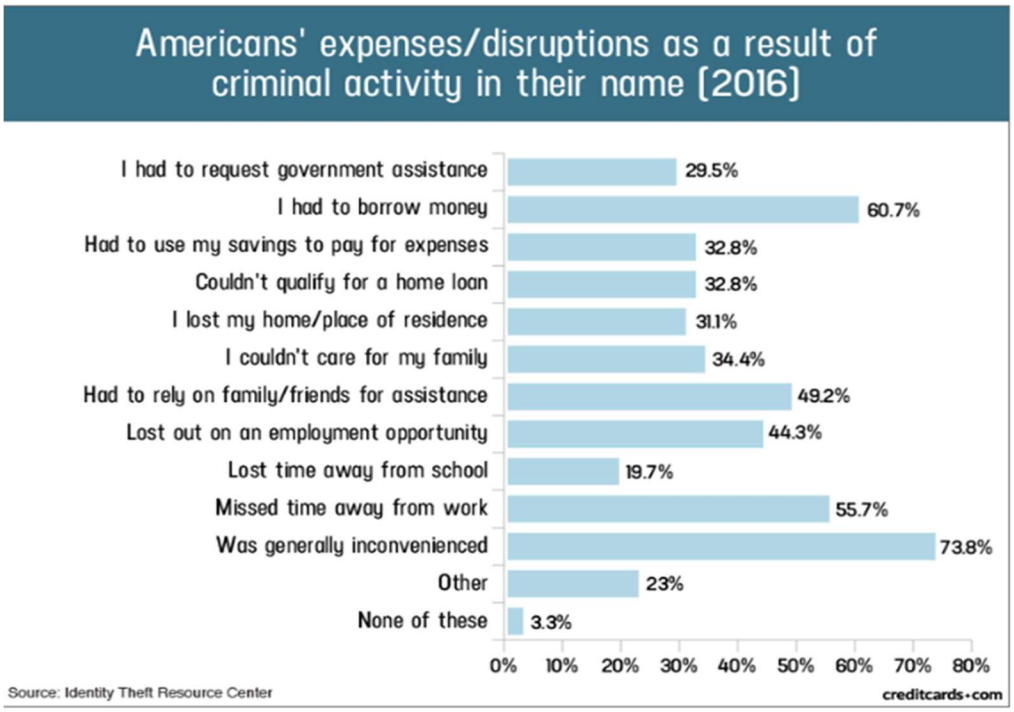
126. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

127. A study by Identity Theft Resource Center shows the multitude of harms caused by

[34] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

[35] *See, e.g.*, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices.

fraudulent use of personal and financial information:[36]



128. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[37] Indeed, the FTC recommends that identity theft victims take several steps and spend time 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 7 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.[38]

[36] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.
[37] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").
[38] *See* https://www.identitytheft.gov/Steps.

C. Diminution of Value of the Private Information

129. PII/PHI is a valuable property right.[39] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

130. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

131. Private Information can sell for as much as $363 per record according to the Infosec Institute.[40]

132. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data was selling on the dark web for $50 and up.[41]

133. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[42] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[43, 44] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[45]

---

[39] *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).

[40] *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/.

[41] https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

[42] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[43] https://datacoup.com/.

[44] https://digi.me/what-is-digime/.

[45] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

134. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the dark web, where it may soon be available and holds significant value for the threat actors.

D. Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

135. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendant offered one year of credit monitoring with Equifax, Experian, or TransUnion.[46]

136. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

137. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

138. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[47] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

---

[46] *See* Exhibit A.

[47] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

139. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

140. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

E. Loss of Benefit of the Bargain

141. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to provide their Private Information, which was a condition precedent to obtain services, and paying Defendant for its services, Plaintiffs, as consumers, understood and expected that they were, in part, paying for services and data security to protect the Private Information required to be collected from them.

142. In fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

F. Injunctive Relief is Necessary to Protect Against Future Data Breaches

143. Moreover, Plaintiffs and Class Members have an interest in ensuring that Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

144. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses and lost time. Also, she suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their Private Information is used;

b. diminution in value of their Private Information;

c. compromise and continuing publication of their Private Information;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen Private Information; and

h. continued risk to their Private Information —which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Private Information.

G. Lack of Compensation

145. Defendant's failed to offer any services to assist Plaintiffs and Class Members in protecting their Private Information.

146. Plaintiffs and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

147. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, imminent, and substantial risk of harm from fraud and identity theft.

148. Further, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach and face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

149. Specifically, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data

Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Monitoring their medical records for fraudulent charges and data;

e. Addressing their inability to withdraw funds linked to compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Placing "freezes" and "alerts" with credit reporting agencies;

h. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i. Contacting financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

150. In addition, Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the property of loss of value damages in related cases.

151. Plaintiffs and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

152. Defendant's delay in identifying and reporting the Data Breach caused additional harm. In a data breach, time is of the essence to reduce the imminent misuse of Private Information. Early

notification helps a victim of a Data Breach mitigate their injuries, and in the converse, delayed notification causes more harm and increases the risk of identity theft. Here, Defendant knew of the breach and waited to formally notify victims. They have yet to offer an explanation for the delay. This delay violates HIPAA and other notification requirements and increases the injuries to Plaintiffs and Class Members.

CLASS ALLEGATIONS

153. Plaintiffs bring this case individually and, pursuant to California Code of Civil Procedure § 382, on behalf of the following class:

> All California citizens whose Private Information was compromised as a result of the Defendant's Data Breach.

154. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

155. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, including by proposing subclasses, based on discovery and prior to moving for class certification.

156. **Numerosity.** The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

157. **Typicality**. Plaintiffs' claims are typical of the claims of the Class Members. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard Private Information. Plaintiffs and Class Members were all patients of Defendant, each having their Private Information obtained by an unauthorized party.

158. **Adequacy of Representation.** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members they seek to

represent; Plaintiffs have retained counsel competent and experienced in complex class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class Members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

159. **Predominant Common Issues of Law and Fact.** This action involves questions of law and fact that are common to the Class Members. Such common questions include, but are not limited to:

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

b. Whether Defendant had a duty to maintain the confidentiality of Plaintiffs and Class Members' Private Information;

c. Whether Defendant breached its obligation to maintain Plaintiffs' and Class Members' medical information in confidence;

d. Whether Defendant was negligent in collecting, storing and safeguarding Plaintiffs' and Class Members' Private Information, and breached its duties thereby;

e. Whether Defendant breached its fiduciary duty to Plaintiffs and Class Members;

f. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

g. Whether Defendant violated the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*.;

h. Whether Defendant violated the California Confidentiality of Medical Information Act, Civ. Code § 56, *et seq*.;

i. Whether Defendant violated the California Customer Records Act, Civ. Code § 1798.80, *et seq*.;

j. Whether Defendant violated the California Unfair Competition Law, Civ. Code § 17200, *et seq*.

k. Whether Defendant invaded Plaintiffs' and Class Members' right to privacy by allowing the disclosure of their Private Information; and

l. Whether Plaintiffs and Class Members are entitled to statutory damages and/or injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

160. **Superiority.** A class action is superior to other alternatives for the fair and efficient adjudication of this controversy. Absent a class action, most members of the Class would find the cost of litigating their claims individually to be prohibitively high and would have no effective remedy. Class treatment will conserve judicial resources, avoid waste and the risk of inconsistent rulings, and promote efficient adjudication before a single Judge.

161. **Injunctive and Declaratory Relief.** Defendant has acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant injunctive and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Negligence and Negligence *Per Se*

162. Plaintiffs restate and reallege paragraphs 1 through 161 above as if fully set forth herein.

163. Defendant owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

164. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

165. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing Private Information that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

166. Defendant's duty also arose by operation of statute. The California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*., the Customer Records Act, Cal. Civ. Code § 1798.80, *et seq*., and the Confidentiality of Medical Information Act, Cal. Civ. Code § 56 *et seq.*, impose a duty on Defendant to implement and maintain reasonable security procedures and practices to safeguard and protect against unauthorized disclosure of personal information.

167. Defendant holds itself out as a trusted provider of healthcare, and thereby assumes a duty to reasonably protect its patients' information. Indeed, Defendant, as a direct health care provider, was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

168. Defendant breached the duties owed to Plaintiffs and Class Members and thus was negligent. Defendant breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; and (f) failing to detect the breach at the time it began or within a reasonable time thereafter.

169. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

170. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant or failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

171. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect the Private Information and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach involving the Private Information of its patients.

172. Plaintiffs and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

173. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

174. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act was intended to guard against.

175. Defendant violated its own policies by actively disclosing Plaintiffs' and Class Members' PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PHI; failing to maintain the confidentiality of Plaintiffs' and the Class Members' records; and by failing to provide timely notice of the breach of PHI to Plaintiffs and the Class.

176. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Loss of their privacy and confidentiality in their PHI;

j. The erosion of the essential and confidential relationship between Defendant – as a healthcare provider– and Plaintiffs and Class Members as its patients; and

k. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received.

177. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION

Violation of the California Consumer Privacy Act

Civ. Code § 1798.100, *et seq*. ("CCPA")

178. Plaintiffs Castro, Friedrich, South, and Zapata (for purposes of the second cause of action, "Plaintiffs") restate and reallege paragraphs 1 through 161 above as if fully set forth herein.

179. In 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. The CCPA imposes a duty on businesses that maintain personal information of California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement the appropriate procedures which resulted in the Data Breach.

180. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

181. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper."

182. Plaintiffs and Class Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in § 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

183. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

184. The Private Information compromised in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiffs' and Class Members' names and Social Security numbers.

185. Plaintiffs and Class Members' Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their personal information, including name and contact information, was unlawfully accessed, viewed and obtained by an unauthorized third party.

186. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to protect the Private Information of Plaintiffs' and Class Members. Defendant failed to implement reasonable security procedures to prevent an attack on its server, including its email system, by hackers and to prevent unauthorized access of Plaintiffs' and Class Members' Private Information as a result of this attack.

187. Plaintiffs provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). Defendant responded to Plaintiffs' notices, but did not cure the violation within 30 days thereof. Defendant has yet to cure the violation. Accordingly, Plaintiffs hereby seek all relief available under the CCPA, including damages to be measured as the greater of

actual damages or statutory damages in an amount up to $750 per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

188. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs also seek injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by this Court.

THIRD CAUSE OF ACTION

Violation of the California Confidentiality of Medical Information Act

Civ. Code § 56, *et seq*. ("CMIA")

189. Plaintiffs restate and reallege paragraphs 1 through 161 above as if fully set forth herein.

190. Defendant is a "provider of health care" as defined in Civil Code § 56.06. Defendant is organized for the purpose of providing healthcare. Defendant is based in California and provides healthcare services to citizens of California.

191. Plaintiffs and Class Members are "patients" within the meaning of Civil Code § 56.05(l).

192. Plaintiffs and Class Members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(i), created, maintained, preserved, stored, abandoned, destroyed, or disposed of on or through Defendant's computer networks at the time of the Data Breach.

193. Defendant violated Civil Code § 56.101 by failing to maintain and preserve the confidentiality of Plaintiffs' and Class Members' medical information.

194. In violation of Civil Code § 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and Class Members' medical information in a manner that failed to preserve the security of that information and breached its confidentiality. As a result, Plaintiffs' and Class Members' confidential information and records were negligently obtained by hackers in the Data Breach.

195. Medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as defined by Civil Code § 56.101(c).

196. That the information obtained in the breach was viewed by unauthorized individuals is evidenced by the fact that the personal information was exfiltrated by hackers.

197. In violation of Civil Code § 56.101(b)(1)(A), Defendant's electronic health record systems or electronic medical record systems failed to protect and preserve the integrity of electronic medical information.

198. Defendant also violated Civil Code §56.36(b) by negligently releasing Plaintiffs' and Class Members' confidential information in the Data Breach.

199. Defendant's wrongful conduct, actions, inaction, omissions, and want of ordinary care violated the CMIA and directly and proximately caused the Data Breach. Plaintiffs and Class Members consequently have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their medical information; (2) loss of the opportunity to control how their medical information is used; (3) diminution in the value and use of their medical information entrusted to Defendant with the understanding that Defendant would safeguard it against theft and not allow it to be accessed and misused by third parties; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identity theft and misuse of their medical information; (5) continued undue risk to their medical information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their medical information being stolen in the Data Breach.

200. Plaintiffs and Class Members were injured and have suffered damages, as described above, from Defendant's negligent release of their medical information in violation of Civil Code §§ 56.36, and 56.101, and accordingly are entitled to relief under Civil Code 56.36, including actual damages, nominal statutory damages of $1,000, injunctive relief, and attorney fees, expenses, and costs.

FOURTH CAUSE OF ACTION

Violation of the California Customer Records Act

Civ. Code § 1798.80, *et seq*. ("CCRA")

201. Plaintiffs restate and reallege paragraphs 1 through 161 above as if fully set forth herein.

202. Plaintiffs and Class Members are "customers" within the meaning of Civil Code § 1798.80(c), as they provided personal information to Defendant for the purpose of obtaining services.

203. Defendant is a "business" within the meaning of Civil Code § 1798.80(a).

204. The CCRA provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California . . . whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person . . . in the most expedient time possible and without unreasonable delay[.]" Civ. Code § 1798.82.

205. The Data Breach was a breach of security within the meaning of § 1798.82. Private Information stolen in the Data Breach, such as names, dates of birth, medical record numbers, Social Security numbers, health insurance policy numbers, claim information, and limited treatment information, as well as other information, constitutes "personal information" within the meaning of §1798.80(e).

206. As a result of Defendant's unreasonable delay in notifying Plaintiffs and Class Members of the Data Breach, Plaintiffs and Class Members were deprived of an opportunity to take appropriate protective measures. In addition, as a result of the delay, Plaintiffs and Class Members have suffered, and will continue to suffer, economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their personal information; (2) loss of the opportunity to control how their personal information is used; (3) diminution in the value and use of their personal information entrusted to Defendant with the understanding that Defendant would safeguard it against theft and not allow it to be accessed and misused by third parties; (4) out-of-pocket

costs associated with the prevention and detection of, and recovery from, identity theft and misuse of their personal information; (5) continued undue risk to their personal information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

207. Therefore, on behalf of the Class, Plaintiffs seek actual damages under Civil Code § 1798.84(b), injunctive and declaratory relief, and any other relief deemed appropriate by the Court.

FIFTH CAUSE OF ACTION

Violation of the California Unfair Competition Law

Civ. Code § 17200, *et seq*. ("UCL")

208. Plaintiffs restate and reallege paragraphs 1 through 161 above as if fully set forth herein.

209. The California Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200 *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

210. By reason of Defendant's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs and Class Members' PII and PHI, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

211. Defendant has violated the UCL by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to Plaintiffs and Class Members.

212. Defendant's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that Plaintiffs' and Class Members' PII and PHI has been compromised for unauthorized parties to see, use, and otherwise exploit.

213. Defendant's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII and PHI also constitute "unfair" business acts and practices within the meaning of Business & Professions Code sections 17200 *et seq*., in that Defendant's conduct was substantially injurious to Plaintiffs and Class Members, offensive to public policy, immoral, unethical, oppressive and unscrupulous, and the gravity of Defendant's conduct outweighs any alleged benefits attributable to such conduct.

214. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class Members' PII and PHI with knowledge that the information would not be adequately protected; by violating the California Confidentiality Of Medical Information Act, Cal. Civ. Code § 56.101(a); by violating the other statutes described above; and by storing Plaintiffs' and Class Members' PII and PHI in an unsecure electronic environment in violation of HIPAA and California's data breach statute, Cal. Civ. Code § 1798.81.5, which require Defendant to take reasonable methods of safeguarding Plaintiffs' and Class Members' PII and PHI.

215. Defendant's practices were also unlawful and in violation of Civil Code sections 1798 *et seq*. and Defendant's own privacy policy because Defendant failed to take reasonable measures to protect Plaintiffs' and Class Members' PII and PHI, and failed to take remedial measures such as notifying its users when it first discovered that their PII and PHI may have been compromised.

216. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82 and Cal. Health & Safety Code §1280.15(b)(2).

217. Defendant's business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the PII and PHI they provided to Defendant will remain private and secure, when in fact it has not been maintained in a private and secure manner, and that Defendant would take proper measures to investigate and remediate a data breach, when Defendant did not do so.

218. Plaintiffs and Class Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendant's above- described wrongful actions, inaction, and omissions including, *inter alia*, the unauthorized release and disclosure of their PII and PHI and lack of notice.

219. But for Defendant's misrepresentations and omissions, Plaintiffs and Class Members would not have provided their PII and PHI to Defendant, or would have insisted that their PII and PHI be more securely protected.

220. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiffs and Class Members were injured and lost money or property, including but not limited to the price received by Defendant for its services, the loss of Plaintiffs' and Class Members' legally protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and additional losses as described herein.

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

222. Plaintiffs seek prospective injunctive relief, including improvements to Defendant's data security systems and practices, in order to ensure that such security is reasonably sufficient to safeguard patients' PII and PHI that remains in Defendant's custody, including but not limited to the following:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment patient data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant not transmit PII or PHI via unencrypted email;

f. Ordering that Defendant not store PII or PHI in email accounts;

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner patient data not necessary for provisions of Defendant's services;

h. Ordering that Defendant conduct regular computer system scanning and security checks;

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective patients about the threats they face as a result of the loss of their PII and PHI to third parties, as well as the steps they must take to protect themselves.

223. Unless such Class-wide injunctive relief is issued, Plaintiffs and Class Members remain at risk, and there is no other adequate remedy at law that would ensure that Plaintiffs (and other consumers) can rely on Defendant's representations regarding its data security in the future.

224. Furthermore, in the alternative to all legal remedies sought herein, Plaintiffs, on behalf of the Class, seek monetary relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including but not

limited to restitution to Plaintiffs and Class Members of money or property that Defendant may have acquired by means of its unlawful, and unfair business practices; restitutionary disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices; declaratory relief; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

SIXTH CAUSE OF ACTION

Invasion of Privacy

225. Plaintiffs restate and reallege paragraphs 1 through 161 above as if fully set forth herein.

226. Defendant wrongfully intruded upon Plaintiffs' and Class Members' seclusion in violation of California law. Plaintiffs and Class Members reasonably expected the Private Information they entrusted to Defendant, such as their names, dates of birth, medical record numbers, Social Security numbers, health insurance policy numbers, claim information, and limited treatment information), would be kept confidential from unauthorized third parties.

227. Defendant unlawfully invaded Plaintiffs' and Class Members' privacy rights by:

a. failing to adequately secure their personal information from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about them in a manner highly offensive to a reasonable person; and

c. enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

228. A reasonable person would find it highly offensive that Defendant, having received, collected, and stored Plaintiffs' and Class Members' Private Information such as dates of birth, Social Security numbers, financial account information, and other personal details, failed to protect that information from unauthorized disclosure to third parties.

229. In failing to adequately protect Plaintiffs' and Class Members' Private Information, Defendant acted knowingly and in reckless disregard of their privacy rights. Defendant also knew or

should have known that its ineffective security measures, and their foreseeable consequences, are highly offensive to a reasonable person in Plaintiffs' and Class Members' position.

230. Defendant's unlawful invasions of privacy damaged Plaintiffs and Class Members. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiffs and Class Members suffered mental distress, and their reasonable expectations of privacy were frustrated and defeated.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all other similarly situated, pray for relief as follows:

A. For an Order certifying the Class, and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and state or local laws;

iii. requiring Defendant to delete and destroy the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiffs' and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

vi. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors; requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to train their security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees,

with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and Class Members;

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

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

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

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

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to

provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, treble, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: September 16, 2024.

Respectfully submitted,

/s/ Kristen Lake Cardoso
Kristen Lake Cardoso (SBN 338762)
Jeff Ostrow (*pro hac vice* forthcoming)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
cardoso@kolawyers.com
ostrow@kolawyers.com

Bart D. Cohen (*pro hac vice* pending)
BAILEY GLASSER LLP
1622 Locust Street
Philadelphia, PA 19103
Telephone: (215) 274-9420
bcohen@baileyglasser.com

Daniel Srourian, Esq. (SBN 285678)
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Telephone: (213) 474-3800
daniel@slfla.com

Danielle L. Perry (SBN 292120)
MASON LLP
5335 Wisconsin Avenue, NW
Suite 640
Washington, DC 20015
Telephone: (202) 429-2290
dperry@masonllp.com

Jason M. Wucetich (SBN 222113)
Dimitrios V. Korovilas (SBN 247230)
WUCETICH & KOROVILAS LLP
222 N. Pacific Coast Hwy., Suite 2000
El Segundo, CA 90245
Telephone: (310) 335-2001
jason@wukolaw.com
dimitri@wukolaw.com

David D. Bibiyan (SBN 287811)
Jeffrey D. Klein (SBN 297296)
Henry G. Glitz (SBN 349815)
BIBIYAN LAW GROUP, P.C.
1460 Wilshire Boulevard
Los Angeles, California 90024
Telephone: (310) 438-5555
david@tomorrowlaw.com
jeff@tomorrowlaw.com
henry@tomorrowlaw.com

Counsel for Plaintiffs and the Proposed Class

EXHIBIT A

PALOMAR HEALTH MEDICAL GROUP®

Reimagining Healthcare™

Dear Valued Patient,

On May 5, 2024, Palomar Health Medical Group ("PHMG") identified suspicious activity on certain computer systems within its network which was later determined to be the result of a cybersecurity event. As a result, access to some systems has been interrupted and will continue to be impacted as our investigation and remediation efforts progress. Presently, PHMG phones, faxes, and portal remain non-functional. Our care teams are trained to work through these disruptions and have initiated procedures to ensure patient care delivery continues to be safe and as minimally impacted as possible.

Immediately following the event, PHMG began working with third-party forensics experts to assist in the investigation and remediation process and notified the appropriate

procedures to ensure patient care delivery continues to be safe and as minimally impacted as possible.

Immediately following the event, PHMG began working with third-party forensics experts to assist in the investigation and remediation process and notified the appropriate authorities. PHMG is also investigating what impact, if any, this event had on the security of data within PHMG's environment. PHMG has reached out to our business partners to ensure they are aware of the event and can any steps they deem necessary.

PHMG remains committed to the care of our patients. While we are able to accommodate patients during this time, they may experience delays. We will send frequent email updates to keep them informed.

For further assistance or information please contact our dedicated support team at 800-256-7009 or visit our website at www.phmg.org for updates.

Regards,
Palomar Health Medical Group