IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE: PROSPECT MEDICAL HOLDINGS, INC. DATA BREACH LITIGATION	Case No: 2:23-cv-03216-WB **CLASS ACTION** **JURY TRIAL DEMANDED**

CONSOLIDATED COMPLAINT – CLASS ACTION

Plaintiffs Joshua Stradinger, Mario Robles, Laura Doverspike, Rodney Hoggro, Yolanda Boyle, Latoya Pratcher, Jay Goldstein, Shamoon Khandia, Lorelei Phillips, and Fidel Medina ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this Consolidated Class Action Complaint against Defendant Prospect Medical Holdings, Inc. ("Defendant" or "Prospect") and allege herein, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII")[1] including, but not limited to full names, Social Security numbers, addresses, dates of birth, driver's license numbers, financial information, and protected health information ("PHI") (collectively, PII and PHI are "Private Information"), of

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

hundreds of thousands of current and former patients and employees stemming from a cyberattack of Defendant's network systems on or around late July and/or early August of 2023.

2. Defendant is a large medical group that provides health care services in the states of California, Connecticut, Pennsylvania, Texas, and Rhode Island.

3. To provide these services, and in the ordinary course of Defendant's business, Defendant acquires, possesses, analyzes, and otherwise utilizes Plaintiffs' and Class Members' Private Information.

4. Defendant is legally required to protect personal information from unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction.

5. With this action, Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Plaintiffs and hundreds of thousands of other similarly situated persons in a massive and preventable cyberattack. Between July 31, 2023 and August 3, 2023, cybercriminals infiltrated Defendant's inadequately protected network servers and accessed and exfiltrated highly sensitive Private Information belonging to Plaintiffs and Class Members which was being kept unprotected and unencrypted (the "Data Breach").

6. Plaintiffs further seek to hold Defendant responsible for not ensuring that Defendant maintained the Private Information in a manner consistent with industry standards.

7. On or about September 29, 2023, Defendant notified state Attorneys General and many Class Members about the widespread Data Breach (the "Notice Letter").[2]

8. While Defendant claims to have discovered the Data Breach as early as August 3, 2023, Defendant did not begin informing victims of the Data Breach until September 29, 2023, nearly two months later. Indeed, Plaintiffs and Class Members were wholly unaware of the Data Breach until they received Notice Letters from Defendant. During this time, Plaintiffs and Class Members were unaware that their sensitive Private Information had been compromised, and that

---

[2] Sample Notice Letter available at the Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/c4f1f925-6136-45dd-99fa-6c92cab12031/3fbe64de-72d7-498f-a271-193fed587811/document.html (last visited Mar. 13, 2024).

they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

9. The Notice Letter provides no further information regarding the Data Breach and only recommends how victims can place a fraud alert or credit freeze on their account and how to sign up for the limited, and abbreviated identity monitoring services Defendant offered to only certain Class Members in response to the Data Breach. The Notice Letter does not explain how the Data Breach occurred, what steps Defendant took following the Data Breach, whether Defendant made any changes to its data security, or most importantly, whether Plaintiffs' and Class Members' Private Information remains in the possession of criminals.

10. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

11. By acquiring, utilizing, and benefiting from Plaintiffs' and Class Members' Private Information for its business purposes, Defendant owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiffs and Class Members. These duties required Defendant to design and implement adequate data security systems to protect Plaintiffs' and Class Members' Private Information in its possession and to keep Plaintiffs' and Class Members' Private Information confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

12. Defendant breached these duties by failing to implement adequate data security measures and protocols to properly safeguard and protect Plaintiffs' and Class Members' Private Information from a foreseeable cyberattack on its systems that resulted in the unauthorized access and theft of Plaintiffs' and Class Members' Private Information.

13. Currently, the full extent of the types of Private Information, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant, its agents, counsel, and forensic security vendors at this phase of the litigation.

14. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable

measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Plaintiffs' and Class Members' Private Information was compromised through disclosure to an unknown and unauthorized criminal third party.

15. Upon information and belief, Defendant breached its duties and obligations 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 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.

16. Based on the type of sophisticated and targeted criminal activity, the type of Private Information involved, and Defendant's admission that the Private Information was accessed, it can be concluded that the unauthorized criminal third party was able to successfully target Plaintiffs' and Class Members' Private Information, infiltrate and gain access to Defendant's network, and exfiltrate Plaintiffs' and Class Members' Private Information, including full names, Social Security numbers, addresses, dates of birth, driver's license numbers, and financial information, for the purposes of utilizing or selling the Private Information for use in future fraud and identity theft related cases.

17. The Personal Information exfiltrated from Defendant's systems has been published and offered for sale on the dark web for 50 bitcoin, approximately $1.3 million, and includes approximately 2.3 terabytes of data accessed and exfiltrated from Defendant's servers. This

information includes the Social Security numbers, passport data, patient medical files, financial and legal documents, and other private information of 500,000 individuals.[3]

18. As a result of Defendant's failures and the Data Breach, Plaintiffs' and Class Members' identities are now at a current and substantial imminent and ongoing risk of identity theft and shall remain at risk for the rest of their lives.

19. As Defendant instructed, advised, and warned in its Notice Letter discussed below, 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 include into the future: (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 and mitigating against the imminent risk of identity theft.

20. 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; (e) loss of time heeding Defendant' warnings and following its instructions in the Notice Letter; (g) deprivation of value of their Private Information; (h) invasions of their privacy; and (i) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant failed to undertake appropriate and adequate measures to protect it.

21. On behalf of themselves and Class Members, Plaintiffs bring causes of action for negligence, negligence per se, breach of express and implied contractual duties, unjust enrichment,

---

[3] https://www.cybersecuritydive.com/news/prospect-medical-data-stolen/691945/ (last visited Oct. 3, 2023)

and common law invasion of privacy. Plaintiffs also bring claims on behalf of a California subclass for violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, the California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*, violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*, and for invasion of privacy based on the California Constitution, Art. 1, § 1. Plaintiffs seek, among other things, compensatory damages, statutory damages, injunctive relief, attorneys' fees, and costs of suit.

II. PARTIES

22. Plaintiff Joshua Stradinger is a natural person and citizen of the State of California residing therein.

23. Plaintiff Mario Robles is a natural person and citizen of the State of California residing therein.

24. Plaintiff Laura Doverspike is a natural person and citizen of the State of California residing therein.

25. Plaintiff Rodney Hoggro is a natural person and citizen of the State of California residing therein.

26. Plaintiff Yolanda Boyle is a natural person and citizen of the State of California residing therein.

27. Plaintiff Latoya Pratcher is a natural person and citizen of the State of California residing therein.

28. Plaintiff Jay Goldstein is a natural person and citizen of the State of California residing therein.

29. Plaintiff Shamoon Khandia is a natural person and citizen of the State of California residing therein.

30. Plaintiff Lorelei Phillips is a natural person and citizen of the State of California residing therein.

31. Plaintiff Fidel Medina is a natural person and citizen of the State of California residing therein.

32. Defendant Prospect Medical Holdings, Inc. is a corporation organized and existing under the laws of the State of Delaware, with corporate headquarters located at 3415 S. Sepulveda Blvd., Los Angeles, CA 90034.

33. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

34. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

35. Jurisdiction if proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (i) there are more than 100 Class Members; (ii) the aggregate amount in controversy exceeds five million dollars ($5,000,000), exclusive of interest and costs; and (iii) some Class Members are citizens of states different than Prospect.

36. This Court has personal jurisdiction over Prospect because it regularly and systematically transacts business in the Commonwealth of Pennsylvania, such that it can reasonably anticipate defending a lawsuit here. Moreover, this Court has jurisdiction over Prospect because its acts and omissions affected Plaintiffs' property interests within Pennsylvania.

37. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events of omissions giving rise to these claims occurred in this district, and/or a substantial part of property that is the subject of this action is situated in this district.

IV. FACTUAL ALLEGATIONS

38. Defendant is a medical group of more than 11,000 physicians and 18,000 employees providing health care services at 16 different hospitals across 5 states. Defendant provides comprehensive health care services to its approximately 600,000 members.

39. Upon information and belief, Defendant provides a HIPAA Notice to every patient upon request.

40. As a condition of providing medical care and medical billing, Defendant compiles, retains and stores its patients and customers sensitive information including to full names, Social Security numbers, addresses, dates of birth, driver's license numbers, financial information, diagnosis information, lab results, prescription information, treatment information, health insurance information, claims information, and medical record numbers.

41. Defendant has served thousands of individuals since its founding and has created and maintains a massive repository of Personal Information, acting as a particularly lucrative target for data thieves looking to obtain, misuse, or sell patient data.

42. In the ordinary course of its business, Defendant maintains the Private Information of its patients, customers, current and past employees, and others including but not limited to full names, Social Security numbers, addresses, dates of birth, driver's license numbers, and financial information.

43. Additionally, Defendant may receive Private Information from other individuals and/or organizations including Plaintiffs' and Class Members' employers, insurance carriers, and in connection with enrollment in employee insurance and retirement benefit plans.

44. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to consumers, Defendant, upon information and belief, promises to, among other things: keep protected health information private; comply with healthcare industry standards related to data security and Private Information, inform consumers of its legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to medical care and treatment, and, provide adequate notice to individuals if their Private Information is disclosed without authorization.

45. As a HIPAA covered business entity (*see infra*), Prospect is required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

46. However, Prospect Medical did not maintain adequate security to protect its systems from infiltration by cybercriminals, and it waited nearly 2 months to disclose the Data Breach publicly.

47. By obtaining, collecting, using, and deriving a benefit from Plaintiffs and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

48. At every step, Defendant stores Plaintiffs' and Class Members' sensitive Private Information and has a duty to protect that Private Information from unauthorized access.

49. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

50. Plaintiffs and Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use their Private Information solely for proper business and healthcare related services and purposes, and to prevent the unauthorized disclosure of their Private Information.

Prospect Medical is a HIPAA Covered Entity

51. Prospect is a HIPAA covered entity that provides healthcare and medical services. As a regular and necessary part of its business, Prospect collects and custodies the highly sensitive Private Information of its patients and clients' patients. Prospect is required under federal and state law to maintain the strictest confidentiality of the patient's Private Information that it requires, receives, and collects, and Prospect Medical is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

52. As a HIPAA covered entity, Prospect is required to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including

by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

53. Due to the nature of Prospet's business, which includes providing a range of medical services, Prospect would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

54. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Prospect assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

55. Plaintiffs and Class Members were current and former patients, customers, employees, and contractors whose Private Information was maintained by Prospect, or who received health-related or other services from Prospect, and directly or indirectly entrusted Prospect Medical with their Private Information.

56. Plaintiffs and the Class Members relied on Prospect to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information. Plaintiffs and Class Members reasonably expected that Prospect would safeguard and keep their Private Information confidential.

57. As described throughout this Complaint, Prospect did not reasonably protect, secure, or store Plaintiffs' and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Prospect maintained. Consequently, cybercriminals circumvented Prospect's security measures, resulting in a significant data breach.

The Rhysida Ransomware Gang Claims Responsibility for the Ransomware Attack

58. An October 1, 2023 article in the Hartford Courant, *Inside the cyberattack at Prospect Medical Holdings CT Hospitals*,[4] provided a far more ominous report of the ransomware impact. According to this article, Prospect first reported a cyberattack to the Connecticut public health department on August 3, 2023 stating the attack occurred at 4:30 a.m. that day. The article states that for 17 days in August, Manchester Memorial Hospital was so crippled by a cyberattack that officials notified emergency services in eastern Connecticut they could not take patients, forcing crews to divert people to hospitals as far away as Massachusetts.

59. The article painted the three Prospect Connecticut hospitals as disorganized and unprepared, and even teetering on financial collapse as a result of the cyberattack. Prospect's IT preparedness was called into question, mainly for its ability to recover. A professor of biomedical informatics from the University of Texas Health Science Center, Dean Sittig, discussed the challenges in recovering from a cyber-attack for a health care provider: "I've seen places take a month, even six weeks," Sittig said. "A lot of it has to do with how your networks are configured, how prepared you are and what sort of backups you have in place. In a ransomware (attack), they lock part of your computer. If you don't have a backup of that, you're in bad shape."

60. On August 24, 2023, on ransomlook.io, Rhysida posted a data set for Prospect Medical Holdings. The data set published reveals that the Prospect Medical data was broken into two data sets, with the publicly available corpus sized at 1.1 TB and 894,676 files. Further, Rhysida indicated that they have already sold more than half of the data published on the dark web. The Prospect data published on the dark webs includes, but is not limited to, copies of driver's licenses, U.S. Passports, Social Security cards, patient statements and other confidential information.

61. On September 11, 2023, on the Databreaches.net blog[5], a blogger named Dissent, posted Rhysida claims responsibility for attack on two U.S. health systems. According to the post,

---

[4] https://www.courant.com/2023/12/27/inside-the-cyberattack-at-prospect-medical-holdings-ct-hospitals
[5] https://www.databreaches.net/rhysida-claims-responsibility-for-attacks-on-two-u-s-health-systems

on August 3, Prospect disclosed a ransomware attack that affected some of its 16 hospitals and 10 clinics, including three hospitals in Connecticut and hospitals run by Crozer Health. Although they have made some progress with recovery, a note on their website today states, “Prospect Medical Holdings, along with all Prospect Medical facilities, is experiencing a systemwide outage. We are working to resolve the issue as soon as possible and regret any inconvenience.”

62. For its part, Rhysida ransomware gang claimed responsibility for the attack, stating, “They kindly provided: more than 500000 SSN, passports of their clients and employees, driver’s licenses, patient files (profile, medical history), financial and legal documents!!! If you are interested in our partner’s confidential documents, you will be able to purchase them too!!! Total 1TB unique files, as well as 1.3TB SQL database.” Rhysida claims to have leaked 45% of all of the files they exfiltrated from Prospect Medical Holdings that they had not yet sold.

<u>The Data Breach and Notice Letter</u>

63. Between July 31, 2023 and August 3, 2023, Prospect Medical detected unauthorized access to certain computer systems within its network environment. The unauthorized access was the result of a cybersecurity attack.[6]

64. Prospect took steps to secure its network systems and investigated the nature and scope of the incident with the consultation of third-party cybersecurity professionals.[7]

65. Through its investigation, Prospect determined that its network and servers were subject to a cyberattack that impacted its network resulting in information on its network being accessed and acquired without authorization.[8]

66. Upon information and belief, Plaintiffs’ and Class Members’ Private Information was exfiltrated and stolen in the attack.

67. Furthermore, the investigation determined that the accessed systems contained Private Information belonging to Plaintiffs and Class Members. Upon information and belief, this

---

[6] *See* Notice Letter
[7] *Id.*
[8] *Id.*

Private Information was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

68. The type of Private Information accessed by the unauthorized actor in the Data Breach includes full names, Social Security numbers, addresses, dates of birth, driver's license numbers, and financial information diagnosis information, lab results, prescription information, treatment information, health insurance information, claims information, and medical record numbers.[9]

69. While Prospect Medical stated in the Notice Letter that the Data Breach occurred between July 31, 2023 and August 3, 2023, Prospect did not begin notifying victims until September 29, 2023, almost two months after Prospect Medical discovered the Data Breach occurred.[10]

70. Defendant had obligations created by contract, industry standards, HIPAA, common law, and its own promises and representations to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

71. Plaintiffs and Class Members provided their Private Information directly, or indirectly, to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

72. Through its Notice Letter, Prospect also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to take steps to mitigate their risk of identity theft, such as reviewing financial accounts, and reviewing credit reports for possible fraud.

73. Prospect has offered abbreviated, non-automatic credit monitoring services to victims demonstrating its knowledge of the harm posed to Plaintiffs and Class Members as a result of the Data Breach. However, the credit monitoring offered does not come close to adequately

[9] *Id.*
[10] *Id.*

addressing the lifelong harm that victims face following the Data Breach. Indeed, the Data Breach involves Private Information that cannot be changed, such as Social Security numbers and PHI.

74. Beginning on or around September 29, 2023, Defendant issued Notice Letters to Plaintiffs and Class Members. In total, Defendant notified at least 190,492 individuals.[11]

75. The Notice Letters sent to Plaintiffs and Class Members stated sensitive information including full names, Social Security numbers, addresses, dates of birth, driver's license numbers, and financial information were accessed and exfiltrated in the Data Breach.

76. As a result of the Data Breach, Plaintiffs and hundreds of thousands of Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

77. Defendant waited almost two months to disclose the Data Brach to Plaintiffs and Class Members. As a result of this delay, Plaintiffs and Class Members had no idea their Private Information had been compromised in the Data Breach, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

78. Defendant's failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Private Information.

79. This Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiffs and Class Members.

80. As a HIPAA covered entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which Prospect was aware and

---

[11] See *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/c4f1f925-6136-45dd-99fa-6c92cab12031.shtml (last visited Mar. 1, 2024).

knew it had a duty to guard against. It is well-known that healthcare businesses such as Defendant, which collect and store the confidential and sensitive PII/PHI of thousands of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

81. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiffs and Class Members.

82. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect its patients' Private Information or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' and consumers' Private Information.

83. Plaintiffs and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their Private Information which includes information that is static, does not change, and can be used to commit myriad financial crimes.

84. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use their Private Information for authorized purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand Defendant safeguard their Private Information.

85. The unencrypted Private Information of Plaintiffs and Class Members has been offered for sale on the dark web as is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. In turn, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

86. Defendant did not use reasonable security procedures and practices appropriate to

the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information.

87. Due to Prospect Medical's inadequate security measures and its delayed notice to victims, Plaintiffs and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

The Data Breach Was Foreseeable

88. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

89. At all relevant times, Prospect knew, or should have known, that Plaintiff, and Class Members' Private Information was a target for malicious actors. Despite such knowledge, Prospect failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyberattacks that Prospect should have anticipated and guarded against.

90. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiffs and Class Members.

91. In light of recent high profile data breaches at other health care providers, Defendant knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

92. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[12]

[12] *2022 Breach Barometer*, PROTENUS, *see* https://blog.protenus.com/key-takeaways-from-the-2022-breach-barometer (last visited Mar. 1, 2024).

93. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[13]

94. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

95. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[14]

96. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[15] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[16] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident in 2010, and that a

[13] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available at: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited Mar. 1, 2024).

[14] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited Mar. 1, 2024).

[15] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited Mar. 1, 2024).

[16] *Id.*

majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[17]

97. Cyberattacks on medical systems like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[18]

98. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[19]

99. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[20]

100. Patient records, like those stolen from Prospect, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[21]

---

[17] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited Mar. 1, 2024).
[18] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Mar. 1, 2024).
[19] https://www.hipaajournal.com/why-do-criminals-target-medical-records/(last visited Mar. 1, 2024).
[20] See *id.*
[21] See *id*.

101. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

102. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[22]

103. Prospect was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[23]

104. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[24]

105. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class Members.

106. The U.S. Department of Health and Human Services and the Office of Consumer

---

[22] *See* Maria Henriquez*, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack*

[23] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820 (last visited Mar. 1, 2024).

[24] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Mar. 1, 2024).

Rights urges the use of encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[25]

107. As a HIPAA covered entity, Prospect Medical should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

Defendant Fails to Comply with FTC Guidelines

108. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

109. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[26] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[27]

110. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex

[25] https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops (last visited Mar. 1, 2024).
[26] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 1, 2024).
[27] *Id*.

passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

111. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating 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 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

112. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

113. Defendant failed to properly implement basic data security practices.

114. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

115. Defendant was at all times fully aware of its obligation to protect the Private Information of customers and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Prospect Medical Fails to Comply with Industry Standards

116. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

117. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to; educating all

employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

118. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

119. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

120. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Prospect Medical's Conduct Violates HIPAA Obligations to Safeguard Private Information

121. As an emergency medical services provider, Prospect Medical is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

122. HIPAA requires covered entities to protect against reasonably anticipated threats

to the security of sensitive patient health information.

123. Prospect Medical is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[5] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

124. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

125. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

126. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

127. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

128. The Data Breach resulted from a combination of insufficiencies that demonstrate Prospect Medical failed to comply with safeguards mandated by HIPAA regulations.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

129. Cyberattacks and data breaches at healthcare companies and partner companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

130. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[28]

131. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[29]

132. 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 face "substantial costs and time to repair the damage to their good name and credit record."[30]

133. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, 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 otherwise harass or track the victim. 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

[28] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited Mar 1. 2024).

[29] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[30] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited Mar. 1, 2024).

whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

134. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[31]

135. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

136. 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.

137. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[32]

138. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that 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.

---

[31] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Mar. 1, 2024).

[32] *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).

139. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

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

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

See GAO Report, at p. 29.

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

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

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

144. Private Information can sell for as much as $363 per record according to the Infosec Institute.[33] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

145. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[34] Such fraud

[33] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Mar. 1, 2024).

[34] *Identity Theft and Your Social Security Number*, Social Security Administration (2018). Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 1, 2024).

may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[35] Each of these fraudulent activities is difficult to detect. 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.

146. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

147. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a 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."[36]

148. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[37]

149. Medical information is especially valuable to identity thieves.

150. 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."[38]

[35] *Id*.

[36] 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 (last visited Mar. 1, 2024).

[37] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 3, 2023).

[38] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Mar. 1, 2024).

151. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase 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.

152. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[39] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[40]

153. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

154. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was on notice of the substantial and foreseeable risk of harm from a data breach, yet Prospect Medical failed to properly prepare for that risk.

155. The Private Information taken from Defendant's systems has been published and offered for sale on the dark web for 50 bitcoin, approximately $1.3 million, and includes approximately 2.3 terabytes of data accessed and exfiltrated from Defendant's servers. This information includes the Social Security numbers, passport data, patient medical files, financial and legal documents, and other private information of 500,000 individuals.[41]

156. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant'sunlawful conduct includes, but is not limited to, the following acts and/or omissions:

---

[39] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong (last visited Mar. 1, 2024).
[40] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited Mar. 1, 2024).
[41] https://www.cybersecuritydive.com/news/prospect-medical-data-stolen/691945/ (last visited Mar. 1, 2024)

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

157. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access Prospect Medical' computer network and systems which contained unsecured and unencrypted Private Information.

158. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant.

<u>Defendant's Response to the Data Breach is Inadequate to Protect Plaintiffs and the Class</u>

159. Defendant failed to inform Plaintiffs and Class Members of the Data Breach in time for them to protect themselves from identity theft.

160. Defendant stated that the Data Breach occurred between July 31, 2023 and August 3, 2023. However, Defendant did not start notifying affected individuals until at least September

29, 2023, nearly 2 months later. Even then, Defendant provided only vague information as to exactly what types of Private Information was accessed and Defendants did not disclose the timeframe which cybercriminals were present on Defendant's network. As a result, Plaintiffs and Class Members are unsure as to the scope of information that was compromised and the risks they face.

161. Defendant's failure to timely notify the victims of its Data Breach meant that Plaintiffs and Class Members were unable to take affirmative measures to prevent or mitigate the resulting harm.

Plaintiffs' and Class Members' Damages

162. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiffs and Class Members have all suffered damages and will face a substantial risk of additional injuries for the rest of their lives. Yet, to date, Defendant has merely offered to provide certain victims of the Data Breach with limited, abbreviated subscriptions to identity monitoring services. This does nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered. Nor will it prevent additional harm from befalling Plaintiffs and Class Members as a result of the Data Breach. And at the conclusion of these limited subscriptions, victims will be required to pay for such services out of their own pocket.

163. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

164. Plaintiffs' and Class Members' Private Information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

165. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring his accounts for fraudulent activity.

166. Plaintiffs' and Class Members' Private Information was compromised as a direct

and proximate result of the Data Breach.

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

168. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

169. Plaintiffs and Class Members 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.

170. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

171. 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.

172. 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 propriety of loss of value damages in related cases.

173. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Prospect Medical' computer system(s) and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for and agreed to.

174. Plaintiffs and Class Members have spent and will continue to spend significant

amounts of time to monitor their medical accounts and sensitive information for misuse.

175. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. 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. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

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

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for the rest of their lives.

176. Moreover, Plaintiffs and Class Members have an interest in ensuring that their 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.

177. Further, as a result of Defendant's conduct, 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, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

178. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and

Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

Plaintiffs' Experiences

Plaintiff Joshua Stradinger's Experience

179. Prior to the Data Breach, Plaintiff Stradinger obtained services from Defendant.

180. On or around September 29, 2023, Plaintiff Stradinger received a Notice of Security Incident from Defendant.

181. As a result of the Data Breach, Plaintiff Stradinger spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through his unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

182. Additionally, Plaintiff Stradinger is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

183. Plaintiff Stradinger stores any documents containing his PII and PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his few online accounts.

184. Plaintiff Stradinger suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff Stradinger entrusted to Defendant for the purpose of obtaining health care services from Defendant, which was compromised in and as a result of the Data Breach.

185. Plaintiff Stradinger suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

186. Plaintiff Stradinger has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI, in

combination with his name, being placed in the hands of unauthorized third-parties and possibly criminals.

187. Plaintiff Stradinger has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Mario Robles' Experience

188. Prior to the Data Breach, Plaintiff Robles obtained services from Defendant.

189. On or around September 29, 2023, Plaintiff Robles received a Notice of Security Incident from Defendant.

190. As a result of the Data Breach, Plaintiff Robles spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through his unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

191. Additionally, Plaintiff Robles is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

192. Plaintiff Robles stores any documents containing his PII and PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his few online accounts.

193. Plaintiff Robles suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff Robles entrusted to Defendant for the purpose of obtaining health care services from Defendant, which was compromised in and as a result of the Data Breach.

194. Plaintiff Robles suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

195. Plaintiff Robles has suffered imminent and impending injury arising from the

substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI, in combination with his name, being placed in the hands of unauthorized third-parties and possibly criminals. Identity tracking alerts indicate his data has been disseminated on the dark web, making the threat even greater.

196. Plaintiff Robles has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Laura Doverspike's Experience

197. Prior to the Data Breach, Plaintiff Doverspike obtained services from Defendant.

198. On or around September 29, 2023, Plaintiff Doverspike received a Notice of Security Incident from Defendant.

199. As a result of the Data Breach, Plaintiff Doverspike spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through her unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

200. Additionally, Plaintiff Doverspike is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

201. Plaintiff Doverspike stores any documents containing her PII and PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her few online accounts.

202. Plaintiff Doverspike suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that Plaintiff Doverspike entrusted to Defendant for the purpose of obtaining health care services from Defendant, which was compromised in and as a result of the Data Breach.

203. Plaintiff Doverspike suffered lost time, annoyance, interference, and inconvenience

as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

204. Plaintiff Doverspike has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI, in combination with her name, being placed in the hands of unauthorized third-parties and possibly criminals.

205. Since the Data Breach, Plaintiff Doverspike has received fraudulent charges on one of her credit cards from an entity called "Midnight Wonders" that she has no affiliation with, as recently as early December. The charges number no less than three distinct charges totaling a minimum of $139.00. Plaintiff Doverspike has been working to get the fraudulent charges removed from her card.

206. Plaintiff Doverspike has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Rodney Hoggro's Experience

207. On or around September 29, 2023, Plaintiff Hoggro was notified via letter from Defendant that his PHI and/or PII had been accessed because of the Data Beach.

208. Plaintiff Hoggro is an adult individual and, at all times relevant herein, a resident and citizen of the State of California. Plaintiff Hoggro is a victim of the Data Breach. Defendant received Plaintiff Hoggro's PHI/PII in connection with the services he received at the Southern California Hospital at Culver City.

209. As a result, Plaintiff Hoggro's information was among the data an unauthorized third party accessed in the Data Breach.

210. On or about September 14, 2023, Plaintiff Hoggro received written communication from the IRS regarding the filing of a tax return using Plaintiff Hoggro's name and Social Security number. Plaintiff Hoggro is informed and believes that the tax return referred to in this letter was not filed by Plaintiff Hoggro, but rather, an unauthorized recipient of Plaintiff Hoggro's PHI/PII as a result of the Data Breach.

211. On or about December 5, 2023, Plaintiff Hoggro received written communication notifying him of "recently reported student loans." Plaintiff Hoggro has never taken out any student loans. Rather, an unauthorized recipient of Plaintiff Hoggro's PHI/PII obtained student loans in Plaintiff Hoggro's name.

212. Plaintiff Hoggro regularly monitors his credit and identity for fraudulent activity since the Data Breach.

213. As a result of the Data Breach, Plaintiff Hoggro spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through his unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

214. Additionally, Plaintiff Hoggro is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

215. Plaintiff Hoggro stores any documents containing his PII and PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his few online accounts.

216. Plaintiff Hoggro suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff Hoggro entrusted to Defendant for the purpose of obtaining health care services from Defendant, which was compromised in and as a result of the Data Breach.

217. Plaintiff Hoggro suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

218. Plaintiff Hoggro has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI, in combination with his name, being placed in the hands of unauthorized third-parties and possibly criminals.

219. Plaintiff Hoggro has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Yolanda Boyle's Experience

220. Prior to the Data Breach, Plaintiff Boyle obtained services from Defendant.

221. On or around September 29, 2023, Plaintiff Boyle received a Notice of Security Incident from Defendant.

222. As a result of the Data Breach, Plaintiff Boyle spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through her unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

223. Additionally, Plaintiff Boyle is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

224. Plaintiff Boyle stores any documents containing her PII and PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her few online accounts.

225. Plaintiff Boyle suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that Plaintiff Boyle entrusted to Defendant for the purpose of obtaining health care services from Defendant, which was compromised in and as a result of the Data Breach.

226. Plaintiff Boyle suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

227. Plaintiff Boyle has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI, in combination with her name, being placed in the hands of unauthorized third-parties and possibly

criminals.

228. Plaintiff Boyle has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Latoya Pratcher's Experience

229. Prior to the Data Breach, Plaintiff Pratcher obtained services from Defendant. Specifically, prior to July 31, 2023, Plaintiff was a patient within the meaning of subdivision (m) of Cal. Civil Code section 56.05, and received of health care services affiliated with at least one of Defendant's following facilities: Southern California Hospital at Culver City, Southern California Hospital at Hollywood, Southern California Hospital at Van Nuys, Los Angeles Community Hospital, Los Angeles Community Hospital at Norwalk, Los Angeles Community Hospital at Bellflower, and Foothill Regional Medical Center.

230. Shortly after September 29, 2023, Plaintiff Pratcher received a Notice of Data Breach from Defendant. Specifically, Plaintiff Pratcher received a letter, addressed in her first and last name with her mailing address, on "Prospect Medical Holdings, Inc." letterhead, dated September 29, 2023, entitled "Notice of Data Breach," and signed "Don Kreitz[,] SVP Southern California Hospitals," stating in relevant part, "we are writing to tell you about a data incident that involved your information," "Through our ongoing investigation, on September 13, 2023, we determined that an unauthorized party gained access to our IT network between the dates of July 31, 2023 and August 3, 2023," and "Our investigation concluded that some of these files contained your information, such as your name, driver's license number, diagnosis information, lab results, prescription information, treatment information, health insurance information, claims information, medical record number and date of birth."

231. After the Data Breach, Plaintiff Pratcher an experienced an unauthorized attempt to access a credit card account in her name, and experiences an increase in spam emails, and suspicious phone calls and texts. Additionally, Plaintiff Pratcher obtained a report from Experian confirming that some of her compromised data has appeared on the dark web.

232. As a result of the Data Breach, Plaintiff Pratcher spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through her unsolicited emails, verifying the legitimacy of the Data Breach, hiring and communicating with her attorneys, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

233. Additionally, Plaintiff Pratcher is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

234. Plaintiff Pratcher suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that Plaintiff Pratcher entrusted to Defendant for the purpose of obtaining health care services from Defendant, which was compromised in and as a result of the Data Breach.

235. Plaintiff Pratcher suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

236. Plaintiff Pratcher has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI, in combination with her name, being placed in the hands of unauthorized third-parties and possibly criminals.

237. Plaintiff Pratcher has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Jay Goldstein's Experience

238. Prior to the Data Breach, Plaintiff Goldstein obtained services from Defendant.

239. On or around September 29, 2023, Plaintiff Goldstein received a Notice of Security Incident from Defendant.

240. As a result of the Data Breach, Plaintiff Goldstein spent time dealing with the

consequences of the Data Breach, which includes time spent on the telephone and sorting through his unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

241. Additionally, Plaintiff Goldstein is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

242. Plaintiff Goldstein stores any documents containing his PII and PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his few online accounts.

243. Plaintiff Goldstein suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff Goldstein entrusted to Defendant for the purpose of obtaining health care services from Defendant, which was compromised in and as a result of the Data Breach.

244. Plaintiff Goldstein suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

245. Plaintiff Goldstein has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI, in combination with his name, being placed in the hands of unauthorized third-parties and possibly criminals.

246. Plaintiff Goldstein has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Shamoon Khandia's Experience

247. Prior to the Data Breach, Plaintiff Khandia obtained services from Defendant and provided Defendant with his Private Information.

248. On or around October 3, 2023, Plaintiff Khandia received a Notice of Security Incident from Defendant.

249. As a result of the Data Breach, Plaintiff Khandia spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through unsolicited emails and text messages, verifying the legitimacy of the Data Breach, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

250. Since the Data Breach, Plaintiff Khandia has suffered actual injuries. Plaintiff has received emails from Experian notifying him of charges on his Experian credit report that did not belong to Plaintiff.

251. As a result of these fraudulent charges on Plaintiff's credit report, Plaintiff's credit score went down. Consequently, Plaintiff has not sought goods or services requiring credit; instead, Plaintiff uses his debit card.

252. Plaintiff further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

253. In January 2024, Plaintiff Khandia received a phone call from an unknown person claiming to be from 'Capital One' in Chicago, Illinois. While Plaintiff does not have a credit card from Capital One, this unknown person allegedly from Capital One insisted that Plaintiff owed thousands of dollars on his Capital One credit card. Plaintiff has subsequently received text messages regarding this same issue.

254. Upon information and belief, Plaintiff Khandia has spent over twenty (20) hours dealing with the consequences of the Data Breach. This time spent involved calling Defendant Prospect Medical about the Data Breach, calling Plaintiff's bank to inquire about the repercussions to Plaintiff's bank account, consulting Experian to dispute fraudulent charges on his credit report and ascertain the drop in Plaintiff's credit score, monitoring his bank accounts and credit reports, and verifying spam phone calls and text messages.

255. Plaintiff Khandia is very careful about sharing his PII and PHI. He has never

knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

256. Plaintiff Khandia stores any documents containing his PII and PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his few online accounts.

257. Plaintiff Khandia suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff Khandia entrusted to Defendant for the purpose of obtaining health care services from Defendant, which was compromised in and as a result of the Data Breach.

258. Plaintiff Khandia suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

259. Plaintiff Khandia has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI, in combination with his name, being placed in the hands of unauthorized third-parties and possibly criminals.

260. Plaintiff Khandia has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Lorelei Phillips' Experience

261. Prior to the Data Breach, Plaintiff Phillips obtained services from Defendant.

262. On or around September 29, 2023, Plaintiff Phillips received a Notice of Security Incident from Defendant. Ms. Phillips also received a notice in August 2023.

263. As a result of the Data Breach, Plaintiff Phillips incurred a fraudulent charge of $832 on her Home Depot card.

264. Ms. Phillips has received eight (8) letters from different entities denying her from opening accounts that she did not authorize or attempt to open. The letters came from Synchrony Bank, Mattress Brothers, Shell Oil, and Target.

265. Additionally, as a result of the Data Breach, Plaintiff Phillips has spent time dealing

with the consequences of the Data Breach, which includes time spent on the telephone and sorting through her unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

266. Additionally, Plaintiff Phillips is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

267. Plaintiff Phillips stores any documents containing her PII and PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her few online accounts.

268. Plaintiff Phillips suffered actual injury in the form of damages to and diminution in the value of her PII and PHI—a form of intangible property that Plaintiff Phillips entrusted to Defendant for the purpose of obtaining health care services from Defendant, which was compromised in and as a result of the Data Breach.

269. Plaintiff Phillips suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

270. Plaintiff Phillips has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI, in combination with her name, being placed in the hands of unauthorized third-parties and possibly criminals.

271. Plaintiff Phillips has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Fidel Medina's Experience

272. Prior to the Data Breach, Plaintiff Medina obtained services from Defendant.

273. After hearing of the Data Breach, Plaintiff Medina called Prospect Medical's breach hotline and they confirmed that his information was exposed in the breach.

274. Plaintiff Medina has received several letters in the mail informing him that he has been denied loans that he did not apply for (specifically car loans and credit card loans). He didn't realize that these were evidence of fraud because Prospect Medical did not notify him of the breach, so he just discarded them.

275. Plaintiff Medina has over 27 hard inquiries on his credit report that he did not authorize. His credit score dropped over 200 points in September 2023.

276. Since the breach occurred, Plaintiff Medina has noticed an increase in the number of spam calls he receives. Spam calls about loans, short-term loans, and pay advances.

277. As a result of the Data Breach, Plaintiff Medina spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through his unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

278. Additionally, Plaintiff Medina is very careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

279. Plaintiff Medina stores any documents containing his PII and PHI in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his few online accounts.

280. Plaintiff Medina suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that Plaintiff Medina entrusted to Defendant for the purpose of obtaining health care services from Defendant, which was compromised in and as a result of the Data Breach.

281. Plaintiff Medina suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

282. Plaintiff Medina has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI, in

combination with his name, being placed in the hands of unauthorized third-parties and possibly criminals.

283. Plaintiff Medina has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

284. Plaintiffs bring this action on behalf of themselves and all other similarly situated persons pursuant to Federal Rule of Civil Procedure 23, including Rule 23(b)(1)-(3) and (c)(4). Plaintiffs seek to represent the following class and subclasses:

> **Nationwide Class**. All persons in the United States whose personal information was compromised in or as a result of Prospect's data breach on or around July 31, 2023 through August 3, 2023, which was announced on or around September 29, 2023.

> **California Subclass.** All persons residing in California whose personal information was compromised in or as a result of Prospect's data breach on or around July 31, 2023 through August 3, 2023, which was announced on or around September 29, 2023.

Excluded from the classes are the following individuals and/or entities: Defendant and its parents, subsidiaries, affiliates, officers, directors, or employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely request to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

285. Plaintiffs reserve the right to amend or modify the class definitions with greater particularity or further division into subclasses or limitation to particular issues.

286. This action has been brought and may be maintained as a class action under Rule 23 because there is a well-defined community of interest in the litigation and the proposed classes

are ascertainable, as described further below:

a. Numerosity: The potential members of the class as defined are so numerous that joinder of all members of the class is impracticable. While the precise number of Class Members at issue has not been determined, Plaintiffs believe the cybersecurity breach affected hundreds of thousands of individuals nationwide.

b. Commonality: There are questions of law and fact common to Plaintiffs and the class that predominate over any questions affecting only the individual members of the class. The common questions of law and fact include, but are not limited to, the following:

   i. Whether Defendant owed a duty to Plaintiffs and Class Members to exercise due care in collecting, storing, processing, and safeguarding their personal information;

   ii. Whether Defendant breached those duties;

   iii. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the personal information of class members;

   iv. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and class members' personal information;

   v. Whether Defendant knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class Members' personal information secure and prevent loss or misuse of that personal information;

   vi. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

   vii. Whether Defendant caused Plaintiffs and Class Members damages;

   viii. Whether the damages Defendant caused to Plaintiffs and Class Members includes the increased risk and fear of identity theft and fraud resulting from the access and exfiltration, theft, or disclosure of their personal information;

ix. Whether Plaintiffs and Class Members are entitled to credit monitoring and other monetary relief;

x. Whether Defendant's failure to implement and maintain reasonable security procedures and practices constitutes negligence;

xi. Whether Defendant's failure to implement and maintain reasonable security procedures and practices constitutes negligence per se;

xii. Whether Defendant's failure to implement and maintain reasonable security procedures and practices constitutes violation of the Federal Trade Commission Act, 15 U.S.C. § 45(a);

xiii. Whether Defendant's failure to implement and maintain reasonable security procedures and practices constitutes violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; and

xiv. Whether the California subclass is entitled to actual pecuniary damages under the private rights of action in the California Customer Records Act, Cal. Civ. Code § 1798.84 and statutory damages under the California Confidentiality of Medical Information Act, Civ. Code § 56, and the proper measure of such damages and/or statutory damages.

c. Typicality. The claims of the named Plaintiffs are typical of the claims of the Class Members because all had their personal information compromised as a result of Defendant's failure to implement and maintain reasonable security measures and the consequent Data Breach.

d. Adequacy of Representation. Plaintiffs will fairly and adequately represent the interests of the class. Counsel who represent Plaintiffs are experienced and competent in consumer and employment class actions, as well as various other types of complex and class litigation.

e. Superiority and Manageabilty. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of all Plaintiffs is not practicable, and questions of law and fact common to Plaintiffs predominate over any questions affecting only Plaintiff. Each Plaintiff has been damaged and is entitled to recovery by reason of Defendant's unlawful failure to adequately safeguard their data. Class action treatment will allow those similarly situated persons to litigate their claims in the manner that is most efficient and economical for the parties and the judicial system. As any civil penalty awarded to any individual class member may be small, the expense and burden of individual litigation make it impracticable for most class members to seek redress individually. It is also unlikely that any individual consumer would bring an action solely on behalf of himself or herself pursuant to the theories asserted herein. Additionally, the proper measure of civil penalties for each wrongful act will be answered in a consistent and uniform manner. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action, as Defendant's records will readily enable the Court and parties to ascertain affected companies and their employees.

287. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the class as a whole.

288. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of the matters and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, processing, using, and safeguarding their personal information;

b. Whether Defendant breached that legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, processing, using, and safeguarding their personal information;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information comprised in the breach; and

e. Whether Class Members are entitled to actual damages, credit monitoring, injunctive relief, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct as alleged herein.

COUNT I
Negligence
(By Plaintiffs and the Nationwide Class Against Defendant)

289. Plaintiffs reallege and incorporate by reference the above allegations contained in paragraphs 1-288 as if fully set forth herein.

290. Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, storing, using, processing, deleting and safeguarding their personal information in its possession from being compromised, stolen, accessed, and/or misused by unauthorized persons. That duty includes a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information that were compliant with and/or better than industry-standard practices. Defendant's duties included a duty to design, maintain, and test its security systems to ensure that Plaintiffs' and Class Members' personal information was adequately secured and protected, to implement processes that would detect a breach of its security system in a timely manner, to timely act upon warnings and alerts, including those generated by

its own security systems regarding intrusions to its networks, and to promptly, properly, and fully notify its customers, Plaintiffs, and Class Members of any data breach

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

292. 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. In fact, not only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their personal information because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendant also knew that it was more likely than not Plaintiffs and other Class Members would be harmed.

293. Defendant's duty also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as Defendant.

294. Various FTC publications and data security breach orders further form the basis of Defendant's duty. According to the FTC, the need for data security should be factored into all business decision making.[42] In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[43] Among other things, the guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is

[42] *Start with Security, A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwith security.pdf

[43] *Protecting Personal Information, A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures. The FBI has also issued guidance on best practices with respect to data security that also form the basis of Defendant's duty of care, as described above.[44]

295. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' personal information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' personal information from disclosure.

296. Defendant also had a duty to safeguard the personal information of Plaintiffs and Class Members and to promptly notify them of a breach because of state laws and statutes that require Defendant to reasonably safeguard personal information, as detailed herein, including Cal. Civ. Code § 1798.80 *et seq.*

297. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiffs and Class Members could take appropriate measures to freeze or lock their credit profiles, cancel or change usernames or passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, develop alternative timekeeping methods or other tacks to avoid untimely or inaccurate wage payments, and take other steps to mitigate or ameliorate the damages caused by Defendant's misconduct.

298. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their personal information.

299. Defendant breached the duties it owed to Plaintiffs and Class Members described

[44] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last viewed Mar. 1, 2024).

above and thus was negligent. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the personal information of Plaintiffs and Class Members; (b) prevent the breach; (c) timely detect the breach; (d) maintain security systems consistent with industry; (e) timely disclose that Plaintiffs' and Class Members' personal information in Defendant's possession had been or was reasonably believed to have been stolen or compromised; (f) failing to comply fully even with its own purported security practices.

300. Defendant knew or should have known of the risks of collecting and storing personal information and the importance of maintaining secure systems, especially in light of the increasing frequency of ransomware attacks. The sheer scope of Defendant's operations further shows that Defendant knew or should have known of the risks and possible harm that could result from its failure to implement and maintain reasonable security measures. On information and belief, this is but one of the several vulnerabilities that plagued Defendant's systems and led to the data breach.

301. Through Defendant's acts and omissions described in this complaint, including Defendant's failure to provide adequate security and its failure to protect the personal information of Plaintiffs and Class members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, Defendant unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' personal information.

302. Defendant further failed to timely and accurately disclose to customers, Plaintiffs, and Class Members that their personal information had been improperly acquired or accessed and/or was available for sale to criminals on the dark web.

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

304. Plaintiffs and Class Members relied on Defendant to keep their personal information confidential and securely maintained, and to use this information for business purposes only, and to make only authorized disclosures of this information.

305. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. As a result of Defendant's failure to protect Plaintiffs' and Class Members' personal information, Plaintiffs' and Class Members' personal information has been accessed by malicious cybercriminals. Plaintiffs' and the Class Members' injuries include:

a. theft of their personal information;

b. costs associated with requested credit freezes;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the 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;

h. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information being placed in the hands of criminals;

i. damages to and diminution of value of their personal information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and the Class Members' data against theft and not allow access and misuse of their data by others;

j. continued risk of exposure to hackers and thieves of their personal 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, along with damages stemming from the stress, fear, and anxiety of an increased risk of identity theft and fraud stemming from the breach;

k. loss of the inherent value of their personal information;

l. the loss of the opportunity to determine for themselves how their personal information is used; and

m. other significant additional risk of identity theft, financial fraud, and other identity-related fraud in the indefinite future.

306. In connection with the conduct descried above, Defendant acted wantonly, recklessly, and with complete disregard for the consequences Plaintiffs and Class Members would suffer if their highly sensitive and confidential personal information, including but not limited to name, company name, address, social security numbers, and banking and credit card information,

was access by unauthorized third parties.

COUNT II
Negligence Per Se
(By Plaintiffs and the Nationwide Class Against Defendant)

307. Plaintiffs reallege and incorporate by reference the above allegations contained in paragraphs 1-288 as if fully set forth herein.

308. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as Defendant. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based on the FTC Act that also created a duty.

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

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

311. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was meant to protect.

312. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the class.

313. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
Breach Of Implied Contract

(On behalf of Plaintiffs and the Nationwide Class)

314. Plaintiffs reallege and incorporate by reference the above allegations contained in paragraphs 1-288 as if fully set forth herein.

315. Plaintiffs and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

316. Plaintiffs and the Class were required to and delivered their Private Information to Defendant as part of the process of obtaining medical services provided by Defendant. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for such services.

317. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant Prospect Medical Holdings, Inc.'s regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

318. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services or Plaintiffs and Class Members.

319. In accepting such information and payment for services, Plaintiffs and the other Class Members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Private Information.

320. In delivering their Private Information to Defendant and providing paying for healthcare services, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard the data as part of that service.

321. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

322. The implied promises include but are not limited to: (1) taking steps to ensure that

any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

323. Plaintiffs and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

324. Had Defendant disclosed to Plaintiffs and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members would not have provided their Sensitive Information to Defendant.

325. Defendant recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

326. Plaintiffs and the other Class Members fully performed their obligations under the implied contracts with Defendant.

327. Defendant breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

328. As a direct and proximate result of Defendant's conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV
Invasion of Privacy
Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On behalf of Plaintiffs and the Nationwide Class Against Defendant)

329. Plaintiffs reallege and incorporate by reference the above allegations contained in

paragraphs 1-288 as if fully set forth herein.

330. To assert claims for intrusion upon seclusion, one must plead (1) that the defendant intentionally intruded into a matter as to which plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

331. Defendant intentionally intruded upon the solitude, seclusion and private affairs of Plaintiffs and Class Members by intentionally configuring their systems in such a way that left them vulnerable to malware/ransomware attack, thus permitting unauthorized access to their systems, which compromised Plaintiffs' and Class Members' personal information. Only Defendant had control over its systems.

332. Defendant's conduct is especially egregious and offensive as they failed to have adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiffs' and Class Members' personal information.

333. At all times, Defendant was aware that Plaintiffs' and Class Members' personal information in their possession contained highly sensitive and confidential personal information.

334. Plaintiffs and Class Members have a reasonable expectation of privacy in their personal information, which also contains highly sensitive medical information.

335. Defendant intentionally configured their systems in such a way that stored Plaintiffs' and Class Members' personal information to be left vulnerable to malware/ransomware attack without regard for Plaintiffs' and Class Members' privacy interests.

336. The disclosure of the sensitive and confidential personal information of thousands of consumers, was highly offensive to Plaintiffs and class members because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

337. Defendant's conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive information, in addition to social norms. Defendant's conduct would be especially egregious to a reasonable person as Defendant publicly disclosed Plaintiffs' and Class Members' sensitive and confidential

personal information without their consent, to an "unauthorized person," i.e., hackers.

338. As a result of Defendant's actions, Plaintiffs and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

339. Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's intrusion upon seclusion and are entitled to just compensation.

340. Plaintiffs and class members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened stress, fear, anxiety, and risk of future invasions of privacy.

COUNT V

Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*

(By California Plaintiffs and the California Class Against Defendant)

341. California Plaintiffs reallege and incorporate by reference the above allegations contained in paragraphs 1-288 as if fully set forth herein.

342. In Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

343. Defendant is a "contractor" within the meaning of Civil Code § 56.05(d) within the meaning of Civil Code § 56.06 and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Defendant, within the meaning of Civil Code § 56.05(k).

344. Plaintiffs and California subclass members are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiffs and California subclass members fear that disclosure of their medical information could

subject them to harassment or abuse.

345. Plaintiffs and California subclass members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network at the time of the unauthorized disclosure.

346. Defendant, through inadequate security, allowed unauthorized third-party access to Plaintiffs' and California subclass members' medical information, without the prior written authorization of Plaintiffs and California subclass members, as required by Civil Code § 56.10 of the CMIA.

347. Defendant violated Civil Code § 56.101 of the CMIA through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the California subclass members. Defendant's conduct with respect to the disclosure of confidential PII and PHI was willful and knowing because Defendant designed and implemented the computer network and security practices that gave rise to the unlawful disclosure.

348. In violation of Civil Code § 56.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and class members' medical information in a manner that failed to preserve and breached the confidentiality of the information contained therein. Plaintiffs' and California subclass member' medical information was viewed by unauthorized individuals including but not limited to, the hackers, individuals who purchased the Private Information on the dark web, and others, as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a). In violation of Civil Code § 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs' and California subclass members' medical information. Plaintiffs' and California subclass members' medical information was viewed by unauthorized individuals, as described above, as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

349. Plaintiffs' and California subclass members' medical information that was the subject of the unauthorized disclosure included "electronic medical records" or "electronic health

records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

350. In violation of Civil Code § 56.101(b)(1)(A), Defendant's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiffs' and California subclass members' medical information was viewed by unauthorized individuals including but not limited to, the hackers, individuals who purchased the Private Information on the dark web, and others, as a direct and proximate result of Defendant's violation of Civil Code § 56.101(b)(1)(A).

351. Defendant violated Civil Code § 56.36 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the California subclass members.

352. As a result of Defendant's above-described conduct, Plaintiffs and California subclass members have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36. 385. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the unauthorized disclosure, and violation of the CMIA, Plaintiffs and California subclass members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud-risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII and PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII and PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

353. Plaintiff, individually and for each member of the Class, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive

damages of up to $3,000 per Plaintiffs and each California subclass member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

COUNT VI
Violation of the California Customer Records Act,
Cal. Civ. Code §§ 1798.80 *et seq.*,
(By California Plaintiffs and the California Subclass Against Defendant)

354. California Plaintiffs reallege and incorporate by reference the above allegations contained in paragraphs 1-288 as if fully set forth herein.

355. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

356. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall 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."

357. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

358. Plaintiffs and members of the California subclass are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant, directly and/or indirectly, for the purpose of obtaining a service from Defendant.

359. The personal information of Plaintiffs and the California subclass at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i)

Social security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

360. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California subclass's personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiffs and the California subclass. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiffs and the California subclass from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiffs' and the California subclass's nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

361. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiffs and the California subclass included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiffs and the California subclass by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

362. As a direct and proximate result of Defendant's acts or omissions, Plaintiffs and the

California subclass were injured and lost money or property including, but not limited to, the loss of Plaintiffs' and the subclass's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

363. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

364. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;
b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
c. If the information is possible to determine at the time the notice is provided, then any of the following:
    i. the date of the breach,
    ii. the estimated date of the breach, or
    iii. the date range within which the breach occurred. The notification shall also include the date of the notice;
d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;
e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;
f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or

California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

365. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiffs and members of the California subclass. On information and belief, to date, Defendant has not sent written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all class members. Because not all members of the class have been notified of the breach, members could have taken action to protect their personal information, but were unable to do so because they were not timely notified of the breach.

366. On information and belief, many class members affected by the breach, have not received any notice at all from Defendant in violation of Section 1798.82(d).

367. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiffs and class members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

368. As a direct consequence of the actions as identified above, Plaintiffs and class members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to §

1798.84(b).

COUNT VII
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code §§ 17200 *et seq.*,
(By California Plaintiffs and the California Subclass Against Defendant)

369. California Plaintiffs reallege and incorporate by reference the above allegations contained in paragraphs 1-288 as if fully set forth herein.

370. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

371. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful and unfair business acts and practices.

372. Defendant' "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiffs' and California subclass members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Defendant data breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56);

c. Defendant's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

373. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, and California common law.

374. Defendant's unlawful and unfair practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and California subclass members' personal information, which was a direct and proximate cause of the Defendant data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Defendant data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, and California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56), which was a direct and proximate cause of the Defendant data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and California subclass members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and California subclass members' personal information; and

375. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56).

376. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

377. As a direct and proximate result of Defendant's unfair and unlawful acts and practices, Plaintiffs and California subclass members were injured and lost money or property, which would not have occurred but for the unfair and unlawful acts alleged herein, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

378. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

379. Plaintiffs and class members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

380. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiffs and California subclass members.

381. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and California subclass members' rights. Past data breaches put Defendant on notice that its security and privacy protections were inadequate.

382. Plaintiffs and California subclass members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair and unlawful business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT VIII
Invasion of Privacy – Cal. Const. Art. 1, § 1
(By California Plaintiffs and the California Subclass Against Defendant)

383. California Plaintiffs reallege and incorporate by reference the above allegations contained in paragraphs 1-288 as if fully set forth herein.

384. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

385. The right to privacy in California's constitution creates a private right of action against private and government entities.

386. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

387. Defendant violated Plaintiffs' and Class Members' constitutional right to privacy by collecting, storing, and disclosing their personal information in which they had a legally protected privacy interest, and in which they had a reasonable expectation of privacy in, in a

manner that was highly offensive to Plaintiffs and Class Members, would be highly offensive to a reasonable person, and was an egregious violation of social norms.

388. Defendant has intruded upon Plaintiffs' and Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential personal information.

389. Defendant's actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the invasion occurred within a zone of privacy protected by the California Constitution, namely the misuse of information gathered for an improper purpose; and (ii) the invasion deprived Plaintiffs and Class Members of the ability to control the circulation of their personal information, which is considered fundamental to the right to privacy.

390. Plaintiffs and Class Members had a reasonable expectation of privacy in that: (i) Defendant's invasion of privacy occurred as a result of Defendant's security practices including the collecting, storage, and unauthorized disclosure of consumers' personal information; (ii) Plaintiffs and Class Members did not consent or otherwise authorize Defendant to disclosure their personal information; and (iii) Plaintiffs and Class Members could not reasonably expect Defendant would commit acts in violation of laws protecting privacy.

391. As a result of Defendant's actions, Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation.

392. Plaintiffs and Class Members suffered actual and concrete injury as a result of Defendant's violations of their privacy interests. Plaintiffs and Class Members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

393. Plaintiffs and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm

to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiffs' and Class Members' privacy.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Classes, 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, and from refusing to issue prompt, complete, any accurate disclosures to 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 its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

   iii. requiring Defendant to delete, destroy, and purge the Private 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 implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

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

vi. 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;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other 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 Private Information, as well as protecting the Private Information 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 its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal 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, but not limited to, actual, consequential, and nominal damages in an amount to be proven at trial, in excess of $5,000,000.

E. Statutory damages pursuant to Cal. Civ. Code § 56.36(b);

F. Reasonable attorneys' fees, including pursuant to Cal. Civ. Pro. Code § 1021.5;

G. For prejudgment interest on all amounts awarded; and

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

Dated: March 14, 2024

Respectfully submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV (*pro hac vice)*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Ste. 200
Nashville, TN 37203
Tel: 615-254-8801
gstranch@stranchlaw.com

M. Anderson Berry, Esq. (*pro hac vice)*
ARNOLD LAW FIRM
865 Howe Avenue
Sacramento, CA 95825
Tel: 916-239-4778
aberry@justice4you.com

Proposed Co-Lead Counsel

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 14th day of March 2024, a true and correct copy of the above and foregoing was filed with the Clerk of Court via the Court's CM/ECF system for electronic service on all counsel of record.

The undersigned hereby also certifies that on the 14th day of March 2024, a true and correct copy of the above and foregoing will be sent via electronic mail to the following:

Luke P. McLoughlin
Alan Kessler
Duane Morris LLP
30 S 17th Street
Philadelphia, PA 19103

Counsel for Defendant

/s/ J.. Gerard Stranch, IV
J. Gerard Stranch, IV