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

[Additonal Counsel listed on signature page]

*Attorneys for Plaintiffs and the Proposed Class*

**SUPERIOR COURT OF THE STATE OF CALIFORNIA**

**FOR THE COUNTY OF LOS ANGELES**

RUDOLPH M. FRANCHI, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

BARLOW RESPIRATORY HOSPITAL,

Defendant.

Case No. 22STCV09016 (LEAD)
Consolidated with Case No. 22STCV17107

[*Assigned for all purposes to Hon. Maren Nelson, Dept. 17*]

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

1. **NEGLIGENCE;**
2. **COMMON LAW INVASION OF PRIVACY;**
3. **CAL. CONST. ART. 1 § 1 INVASION OF PRIVACY**
4. **BREACH OF IMPLIED CONTRACT**
5. **CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE § 56, *et seq*.;**
6. **CALIFORNIA CONSUMER PRIVACY ACT;**
7. **CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200, *et seq*.AND**
8. **DECLARATORY RELIEF.**

**DEMAND FOR JURY TRIAL**

Complaint Filed: March 14, 2022

Plaintiffs Rudolph M. Franchi and Carlos Aragon ("Plaintiffs") bring this Class Action Complaint against Barlow Respiratory Hospital ("Defendant" or "Barlow"), in their individual capacity and on behalf of all others similarly situated, and allege, 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 the Protected Health Information ("PHI"), such as medical and health insurance information, of patients, and its failure to properly secure and safeguard Personally Identifiable Information ("PII") that Defendant required patients, employees, and physicians to provide, including without limitation, first and last names, Social Security numbers, driver's license numbers, financial account information, and online account credentials.

2. Defendant is a hospital located in Los Angeles County that operates as a long-term acute care facility that specializes in weaning chronically and critically ill patients from mechanical ventilation and also treats respiratory diseases and related secondary ailments. Defendant's patients, employees, and physicians entrust it with an extensive amount of their PHI and PII. Defendant retains this information for at least many years.

3. On August 27, 2021, Defendant became aware of a cybersecurity incident that disrupted the operations of its IT systems and subsequently determined that cybercriminals gained unfettered access to Defendant's systems from August 21, 2021 to September 1, 2021 (the "Data Breach"). As a result of the Data Breach, Plaintiffs and at least 9,880 Class Members[1] had their most sensitive personal information accessed, exfiltrated, and published by cybercriminals on the internet, causing them to suffer 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.

4. According to Defendant, the PII compromised and accessed by unauthorized third parties in the Data Breach includes Defendant's current and former patients', employees', and physicians',

[1] *See Cases Currently Under Investigation*, Office for Civil Rights, U.S. Dept. of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited March 12, 2022).

names, contact information, dates of birth, Social Security numbers, and driver's license numbers, as well as PHI such as medical record numbers, treatment information, diagnosis information, dates of service, provider names, financial account information, and health insurance information (collectively, the PII and PHI at issue is "Private Information").

5. This was Defendant's second major data breach since 2019 and Defendant knew or should have known not only of the risk of another attack but the severe consequences to Plaintiffs and Class Members should Defendant fail to safeguard their Private Information.

6. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

7. Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and the utter failure to protect its patients' and employees' sensitive data. Hackers obtained Plaintiffs' and Class Members' PII and PHI because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The risk to these individuals will remain for their respective lifetimes.

8. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

9. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the

Private Information from those risks left that property in a dangerous condition. Defendant did not even take basic precautions by encrypting the Private Information.[2]

10. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Barlow collected and maintained was accessed, exfiltrated, and published by data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, for example, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now, and in the future, closely monitor their financial accounts to guard against identity theft.

13. Plaintiffs and Class Members may also incur out of pocket costs for, for example, purchasing credit monitoring services, identity theft insurance, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

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

15. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and/or PHI; (ii) out-of-pocket expenses

[2] It is clear that the PII exposed in the Data Breach was not encrypted: California law requires entities to notify California residents "whose **unencrypted personal information** was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1) (emphasis added). Defendant notified residents and the California Attorney General of the Data Breach on or about Dec. 30, 2021 and Mar. 4, 2022, evidencing that the exposed data was unencrypted (*see* https://oag.ca.gov/privacy/databreach/list?field_sb24_org_name_value=barlow&field_sb24_breach_date_value%5Bmin%5D%5Bdate%5D=&field_sb24_breach_date_value%5Bmax%5D%5Bdate%5D= (last visited Sept. 14, 2022.)

associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and/or PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (iv) the continued and certainly increased risk to their PII and/or PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

16. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain 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 Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and should be entitled to injunctive and other equitable relief.

17. Plaintiffs bring this action on behalf of all persons whose PII and/or PHI was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

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

///

///

## II. PARTIES

***PLAINTIFF RUDOLPH M. FRANCHI***

19. Plaintiff Rudolph M. Franchi is, and at all times relevant, has been a resident and citizen of Los Angeles, California. Prior to the Data Breach Plaintiff Franchi was a patient of Defendant. Plaintiff Franchi received a letter from Defendant Barlow dated March 4, 2022, on or about that date.

20. The letter notified Plaintiff Franchi that on August 27, 2021, Defendant discovered an "incident" that "disrupted the operations of [its] IT systems." The letter states that a subsequent investigation determined "an unauthorized party gained access to [Defendant's] systems from August 21, 2021 to September 1, 2021. The investigation also determined that the unauthorized party removed some files from [its] systems that contained information pertaining to Barlow patients."

21. The letter from Defendant further informed Plaintiff Franchi that his "name, contact information, date of birth, medical record number, treatment information, diagnosis information, prescription information, date(s) of service, provider name(s), and/or health information" were compromised and accessed by unauthorized third parties in the Data Breach.

22. Upon information and belief, Defendant continues to maintain copies of Plaintiff Franchi's Private Information.

23. Plaintiff Franchi was required to provide his PII and PHI when he was admitted as a patient of Defendant, and Defendant generated additional PHI while he was a patient.

24. Plaintiff Franchi typically takes measures to protect his Private Information and 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.

25. Plaintiff Franchi stores any documents containing his Private Information in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

26. Following, and as a result of, the Data Breach, Plaintiff Franchi has experienced a substantial increase in suspicious scam phone calls and emails, all of which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack.

27. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Franchi made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching the credit monitoring and identity theft protection services offered by Defendant. Plaintiff Franchi has spent at least 5 hours dealing with the Data Breach, valuable time Plaintiff Franchi otherwise would have spent on other activities, including but not limited to work and/or recreation.

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

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

30. Plaintiff Franchi is very concerned about his PII and medical information being accessed and exfiltrated by cybercriminals.

31. If Plaintiff Franchi had known that Defendant would not adequately protect his PII and PHI, he would not have allowed Defendant access to this sensitive and private information.

***PLAINTIFF CARLOS ARAGON***

32. Plaintiff Carlos Aragon is a resident and citizen of California, currently residing in Alhambra, CA. Plaintiff Aragon received Defendant's Notice of Data Breach, dated March 4, 2022, shortly after that date.

33. Defendant's letter informed Plaintiff Aragon that his PII and PHI, including his name, Social Security number, driver's license number, financial account information, online account credentials, medical information, and/or health insurance information, was compromised as a result.

34. Plaintiff Aragon was required to provide and did provide his PII and PHI to Defendant during the course of his employment with Defendant.

35. Plaintiff Aragon typically takes measures to protect his Private Information and 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.

36. Plaintiff Aragon stores any documents containing his Private Information in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.

37. Following, and as a result of, the Data Breach, Plaintiff Aragon has experienced a substantial increase in suspicious scam phone calls and emails, all of which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack

38. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Aragon made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching the credit monitoring and identity theft protection services offered by Defendant. Plaintiff Aragon has spent at least 10 hours dealing with the Data Breach, valuable time Plaintiff Aragon otherwise would have spent on other activities, including but not limited to work and/or recreation.

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

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

41. Upon information and belief, Defendant continues to maintain copies of Plaintiff Aragon's Private Information.

42. If Plaintiff Aragon had known that Defendant would not adequately protect his PII and PHI, he would not have allowed Defendant access to this sensitive and private information.

***DEFENDANT BARLOW RESPIRATORY HOSPITAL***

43. Defendant Barlow Respiratory Hospital is a medical provider headquartered at 2000 Stadium Way, Los Angeles, California 90026.

## III. JURISDICTION AND VENUE

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

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

46. Venue is proper in this Court under California Bus. & Prof. Code § 17203 and Code of Civil Procedure §§ 395(a) and 395.5 because Defendant, and/or its parents or affiliates, is headquartered in this judicial district and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this judicial district.

## IV. FACTUAL ALLEGATIONS

***DEFENDANT'S BUSINESS***

47. Defendant provides post-ICU care for patients who need continued long-term acute care after they are discharged from a short-term acute care hospital. Specifically, Defendant specializes in ventilator weaning, care for medically complex patients, respiratory care, and wound care.

48. Defendant's main campus is the Barlow Respiratory Hospital, a 105-bed, long-term acute care hospital in Los Angeles, California. It also has satellite campuses within both PIH Health Hospital in Whittier, California and Valley Presbyterian Hospital in Van Nuys, California. Although Barlow admits patients from all over Southern California, its primary service area is Los Angeles County, where approximately 94 percent of its patients reside.[3]

49. In the ordinary course of its business Defendant employs staff and physicians to provide care to its patients from whom it collects and maintains sensitive personal and private information as a condition of employment, including but not limited to the Private Information compromised in the Data Breach.

50. Upon information and belief, Defendant made promises and representations to its employees and physicians, including Plaintiff Aragon and employee Class Members, that the PHI and PII collected from them as a condition of employment and/or providing their labor services at Barlow would be kept safe, confidential, and that the privacy of that information would be maintained.

51. Plaintiff Aragon and employee Class Members, as current and former employees and physicians of Defendant, relied on the sophistication of Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff Aragon and Class Members demand security to safeguard their PII and PHI.

52. On information and belief, in the ordinary course of business as a condition of service, Barlow requires patients to provide copious amounts of sensitive personal and private information as a condition of receiving services, including but not limited to the Private Information compromised in the Data Breach.

53. Upon information and belief, Barlow provides each of its patients with a HIPAA compliant notice titled "NOTICE OF PRIVACY PRACTICES" (the "Privacy Notice") that explains how

[3] https://www.barlowhospital.org/documents/content/Community_Health_Needs_Assessment_2020.pdf (last visited March 14, 2022).

Defendant handles its patients' sensitive and confidential information.[4] The Privacy Notice is also posted on Defendant's website.[5]

54. In recognition of Defendant's duty to use reasonable measures to safeguard Private Information, the Privacy Notice states:

> We understand that medical information about you and your health is personal. We are committed to protecting medical information about you. We create a record of the care and services you receive at the hospital. We need this record to provide you with quality care and to comply with certain legal requirements. This Notice applies to all of the records of your care generated by the hospital, whether made by hospital personnel or your personal doctor.[6]

55. The Privacy Notice also acknowledges that Defendant is "required by law" to:

> • Keep your medical information, also known as "protected health information" or "PHI" private;
>
> • Give you this Notice of our legal duties and privacy practices with respect to your PHI;
>
> • Follow the terms of the Notice that are currently in effect; and
>
> • Inform you promptly if a breach occurs that may have compromised the privacy or security of your information.

56. Similarly, the Privacy Policy on Defendant's website states:

> We recognize that you may be concerned about our use and disclosure of your personal information.
> …
> We follow generally accepted industry standards to protect the information submitted to us, both during transmission and once we receive it.
> …
> While we use encryption to protect sensitive information transmitted online, we also protect your information offline. Only employees who need the information to perform a specific job (for example, billing or customer service) are granted

[4] https://www.barlowhospital.org/documents/content/Notice-of-Privacy-Practices-3-2019.pdf (last visited March 12, 2022).

[5] *Id*.

[6] *Id.*

> access to personally identifiable information. The computers/servers in which we store personally identifiable information are kept in a secure environment.[7]

57. 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.

58. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiffs and Class Members, to keep their PHI and PII confidential and to protect it from unauthorized access and disclosure.

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

60. Plaintiffs and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

61. Plaintiffs and Class Members provided their Private Information 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.

***THE CYBERATTACK AND DATA BREACH***

62. On or about August 27, 2021, Barlow identified an "incident" that "disrupted the operations of its IT systems."[8] Over six months later, on or about March 4, 2022, Defendant finally began sending Plaintiffs and other current and former patients, employees, and physicians a *Notice of Data Breach* (the "Notice").

63. According to the Notice, an investigation later determined that that "an unauthorized party gained access to [Defendant's] systems between August 21, 2021 and September 1, 2021. The

[7] https://www.barlowhospital.org/about-barlow/privacy-policy/ (last visited Sept. 12, 2022). Although Defendant claims to "use encryption to protect sensitive information transmitted online," Defendant did not use encryption to safeguard Plaintiffs' and Class Member's PII and PHI stored, and ultimately stolen, on its systems.

[8] https://www.barlowhospital.org/documents/Notice-of-Data-Security-Incident-Barlow-Respiratory-Hospital.pdf (last visited Sept.12, 2022).

investigation also determined that the unauthorized party removed some files from [its] systems."[9] The language in the notices to Class Members and the various Attorneys' General is unequivocal: an "unauthorized party" gained "access" to and "removed" the Private information that included PII and PHI, including, among many other things, "Social Security numbers," "treatment" and "diagnosis information," and other sensitive Private Information.

64. The Notice letter directed Plaintiffs and Class Members to take action to mitigate their damages by, among other things, "review[ing] the statements you receive from your healthcare providers and health insurance plan….[and] reviewing your financial account statements for any suspicious activity."

65. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again have not been shared with Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII and PHI remains protected.

66. The attack was conducted by a criminal group known as "Vice Society."[10]

67. It has been reported that following the Data Breach, Vice Society published patient records on the internet through its "dark web data leak page."[11]

68. Data published online by Vice Society indicates that the Data Breach involved files from as far back as 2001.[12] For example, Vice Society published "1,650 files with consultation notes on named patients that include their personal and medical information in multi-page reports. … [T]he bulk of the reports are dated between 2001 and 2009."[13]

---

[9] *Id.*

[10] https://www.hipaaguidelines101.com/ransomware-gangs-attack-missouri-delta-medical-center-and-barlow-respiratory-hospital/ (last visited March 12, 2022).

[11] https://www.hipaacompliancejournal.com/ransomware-groups-attack-barlow-respiratory-hospital-and-missouri-delta-medical-center/ (last visited March 12, 2022).

[12] https://www.databreaches.net/barlow-respiratory-hospital-recovering-from-breach-but-may-have-a-long-incident-response-road-aheadbarlow-respiratory-hospital-recovering-from-breach-but-long-incident-response-road-ahead/ (last visited March 12, 2022).

[13] *Id.*

69. Current files and reports were also in the online data dump. For example, reporters were able to locate "spreadsheets with information on COVID patients and their responses to treatment."[14] These spreadsheets "contain patients' real names" and other sensitive data.[15] "No password was required to open these files after downloading them."[16]

70. Unauthorized individuals can now easily access the PII and PHI of Plaintiffs and Class Members.

71. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII and PHI for many current and former patients, employees, and physicians, such as encrypting the information or deleting it when it is no longer needed.

***DEFENDANT FAILED TO COMPLY WITH INDUSTRY STANDARDS***

72. Several best practices have been identified that at 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.

73. 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; and training staff regarding critical points.

74. 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-

[14] *Id.*

[15] *Id.*

[16] *Id.*

4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC).

75. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[17]

76. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular

[17] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Sept. 14, 2022).

Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

77. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- Use caution with links and when entering website addresses. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….
- Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- Keep your personal information safe. Check a website's security to ensure the information you submit is encrypted before you provide it….
- Verify email senders. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- Inform yourself. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[18]

78. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

**Secure internet-facing assets**

-Apply latest security updates
-Use threat and vulnerability management
-Perform regular audit; remove privileged credentials;

**Thoroughly investigate and remediate alerts**

-Prioritize and treat commodity malware infections as potential full compromise;

**Include IT Pros in security discussions**

-Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

**Build credential hygiene**

-Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

**Apply principle of least-privilege**

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

**Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[19]

---

[18] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Sept. 14, 2022).

[19] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Sept. 14, 2022).

79. Given that Defendant was storing the PII and PHI of its current and former patients, employees and physicians, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

80. These foregoing frameworks are existing and applicable industry standards for reasonable cybersecurity readiness 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.

81. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII and PHI of an undisclosed amount of current and former employees and physicians, including Plaintiffs and Class Members.

***DEFENDANT KNEW THE PRIVATE INFORMATION ON ITS NETWORK WAS A TARGET***

82. Vice Society reportedly conducted multiple cyberattacks on healthcare providers in the Summer of 2021 before conducting the Barlow cyberattack.[20] Upon information and belief, Vice Society exploited many of the same vulnerabilities in Barlow's network that it had previously exploited to access other healthcare provider networks.

83. Defendant itself suffered a different data breach in November 2019.[21] Defendant's 2019 data breach included similar unauthorized access to information as here: names; Social Security numbers; driver's license numbers; dates of birth; medical record numbers; patient account numbers; treatment information: health insurance information; and medical billing or claims information.[22] In light of the 2019 data breach and recent high-profile data breaches at other companies in the healthcare industry, Defendant knew or should have known that its electronic records, including patients' sensitive PII and PHI, would be targeted by cybercriminals.

84. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued

[20] https://www.hipaaguidelines101.com/ransomware-gangs-attack-missouri-delta-medical-center-and-barlow-respiratory-hospital/ (last visited Sept. 14, 2022).

[21] https://www.prnewswire.com/news-releases/healthcare-resource-group-inc-provides-notice-of-a-data-breach-301037003.html (last visited Sept. 14, 2022).

[22] *Id.*

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."[23]

85. In fact, according to the cybersecurity firm Mimecast, 90 percent of healthcare organizations experienced cyberattacks in the year 2020.[24]

86. Defendant knew and understood unprotected or exposed PII and PHI in the custody of healthcare companies, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII and PHI through unauthorized access.

87. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[25] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[26] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impacts the economy as a whole.[27]

88. Healthcare related data breaches continue to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported

---

[23] *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 Sept. 14, 2022).

[24] *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 (last visited Sept. 14, 2022).

[25] *See* Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/ (last visited Oct. 26, 2021).

[26] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Sept. 14, 2022).

[27] *See id*.

having a significant security incident within the previous 12 months, and most of these known incidents being caused by "bad actors," such as cybercriminals.[28] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[29]

89. The increase in cyberattacks targeting the healthcare industry, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, and particularly to Defendant.

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

91. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

## V. DEFENDANT'S BREACH

92. 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's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

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

---

[28] *See 2019 HIMSS Cybersecurity Survey, available at*: https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Sept. 14, 2022).

[29] *See* Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited Sept. 14, 2022).

b. Failing to adequately protect 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; and;

f. Failing to adhere to industry standards for cybersecurity.

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

94. Accordingly, as outlined below, Plaintiffs and Class Members now face a present and substantially 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.

### A. Cyberattacks And Data Breaches Cause Disruption And Put Consumers At A Present And Substantially Increased Risk Of Fraud And Identity Theft

95. Cyberattacks and data breaches of healthcare providers like Defendant are especially problematic because they can negatively impact the daily lives of individuals affected by the attack.

96. 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.[30]

97. 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.[31]

98. The United States Government Accountability Office released a report in 2007

[30] *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 Sept. 14, 2022).

[31] *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 (last visited Sept. 14, 2022).

regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[32]

99. 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. They do this 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 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.

100. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[33]

101. 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.

102. 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

[32] *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 Sept. 14, 2022).

[33] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/#/Steps (last visited Sept. 14, 2022).

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.

103. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.[34]

104. 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.

105. 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.[35]

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

107. 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.

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

---

[34] *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).

[35] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Sept. 14, 2022).

> [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.[36]

109. 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.

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

111. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come. In fact, Defendant warned impacted patients in the notices about the Data Breach to review all statements from healthcare providers and insurance plans, and to sign up for credit monitoring and identity theft insurance.

112. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[37] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

113. 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.[38] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security

---

[36] *See* GAO Report, at p. 29.

[37] *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 Sept. 14, 2022).

[38] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 14, 2022).

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.[39] 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.

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

115. 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."[40]

116. 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."[41]

117. Medical information is especially valuable to identity thieves.

118. 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.[42] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[43]

---

[39] *Id.* at 4.

[40] 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 Sept. 14, 2022).

[41] 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 Sept. 14, 2022).

[42] *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 Sept. 14, 2022).

[43] 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 Sept. 14, 2022).

119. 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.

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

**B. Defendant's Conduct Violates HIPPA**

121. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities, including Defendant, must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[44]

122. 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 PHI—the type of data Defendant failed to safeguard. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

123. The State of California generally prohibits healthcare providers from disclosing a patient's confidential medical information without prior authorization. California's CMIA (Cal. Civil Code. § 56.10(a)) states that "a provider of health care, health service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care on enrollee or subscriber of a health care service plan without first obtaining an authorization except as provided in subdivision (b) or (c) [of Cal. Civil Code § 56.10]."

124. Defendant's Data Breach resulted from a combination of insufficiencies demonstrating Defendant failed to comply with safeguards mandated by HIPAA regulations. Defendant's security failures include, but are not limited to:

---

[44] *See* HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?, available at:* https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last visited Sept. 14, 2022).

a. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant create, receive, maintain, and transmit, in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information 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);

c. 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);

d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. § 164.308(a)(6)(ii);

e. Failing to protect against any reasonably–anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 C.F.R. § 164.306(a)(2);

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

g. Failing to ensure compliance with HIPAA security standard rules by their workforce, in violation of 45 C.F.R. § 164.306(a)(94);

h. Impermissibly and improperly using and disclosing protected health information that is, and remains, accessible to unauthorized persons, in violation of 45 C.F.R. § 164.502, et seq.; and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c).

125. 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 be factored into all business decision-making.

126. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These 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.[45]

127. 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.[46]

128. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; 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.

129. 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.

130. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL

---

[45] *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 Sept. 14, 2022).

[46] *Id*.

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.")

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

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

133. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

**C. Plaintiffs' and Class Members' Damages**

134. To date, Defendant has done nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

135. Plaintiffs' and Class Members' Private Information was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendant's computer system and removed the Private Information. Upon information and belief, these cybercriminals have published Plaintiffs' and Class Members' Private Information to the internet.

136. Plaintiffs and Class Members' Private Information was compromised and accessed as a direct and proximate result of the Data Breach.

137. Plaintiffs and Class Member suffered harm because Defendant's violated their right to confidentiality under the CMIA. Specifically, Defendant disclosed Plaintiffs' and Class Member's information without authorization or in compliance with exceptions listed in Cal. Civil Code § 56.10(b)-(c).

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

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

140. Plaintiffs and Class Members face the present and substantially increased 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.

141. Plaintiffs and Class Members face the present and substantially increased 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.

142. 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.

143. 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.

144. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service or product that was intended to be accompanied by adequate data security 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 Barlow's computer network and Plaintiffs and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for and agreed to.

145. 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.

146. 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 years to come.

147. 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 or at the very least encrypted.

148. 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—have been disclosed to the world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

## VI. CLASS ALLEGATIONS

149. This action is properly maintainable as a class action. Plaintiffs bring this class action on behalf of himself and on behalf of all others similarly situated pursuant to the Code of Civil Procedure §382, for the following classes defined as:

**All persons residing in the United States to whom Defendant sent a Notice of Data Breach letter informing them of an "incident" which led to access and removal of**

**patients' personally identifying information and protected health information from August 21, 2021 to September 1, 2021 (the "Class").**

**All persons residing in the United States to whom Defendant sent a Notice of Data Breach letter to their California address informing them of an "incident" which led to access and removal of patients' personally identifying information and protected health information from August 21, 2021 to September 1, 2021 (the "California Class").**

150. Separately, Plaintiff Franchi seeks to represent a class of current and former patients defined as:

**All current and former patients of Defendant to whom Defendant sent a Notice of Data Breach letter informing them of an "incident" which led to access and removal of personally identifying information and protected health information from August 21, 2021 to September 1, 2021 (the "Patient Class").**

151. Separately, Plaintiff Aragon seeks to represent a class of current and former employees and physicians of Barlow defined as:

**All current and former employees and physicians of Defendant to whom Defendant sent a Notice of Data Breach letter informing them of an "incident" which led to access and removal of personally identifying information and protected health information from August 21, 2021 to September 1, 2021 (the "Patient Class").**

152. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election 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.

153. Plaintiffs reserve the right under California Rules of Court, rule 3.765 to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

154. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. The Class is apparently identifiable within Defendant's records.

///

155. Commonality and Predominance: Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

b. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

c. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

d. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

e. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

f. Whether Defendant violated the CMIA, Cal. Cod § 56, *et seq*.;

g. Whether Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

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

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

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

156. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other member, was exposed to virtually identical conduct and now suffers from the same violations of the law as other members of the Class.

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

158. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

159. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

160. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could

unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

161. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

162. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

163. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

## FIRST CAUSE OF ACTION
## NEGLIGENCE
**(On Behalf of Plaintiffs and the Class, the Employee Class, and Patient Class)**

164. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

165. Plaintiffs bring this Count on their own behalf and on behalf of the Class, the Employee Class, and the Patient Class (the "Classes" for the purposes of this Count).

166. As condition of employment with and/or providing their labor services to Defendant, Defendant's current and former employees and physicians (including Plaintiff Aragon and Employee Class Members) were obligated to provide Defendant with the sensitive PII and PHI referenced herein.

167. As a condition of receiving healthcare services from Defendant, Defendant's current and former patients (including Plaintiff Barlow and Patient Class Members) were obligated to provide Defendant with the sensitive PII and PHI referenced herein.

168. Plaintiffs and the Classes entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

169. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and the Classes could and would suffer if the PII and PHI were wrongfully disclosed.

170. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiffs and the Classes involved an unreasonable risk of harm to Plaintiffs and the Classes, even if the harm occurred through the criminal acts of a third party.

171. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiffs and the Classes in Defendant's possession was adequately secured and protected.

172. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients', employees', and physicians' PII and PHI that Defendant were no longer required to retain pursuant to regulations.

173. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiffs and the Classes.

174. Defendant's duty to use reasonable security measures arose as a result of the contractual relationship that existed between Defendant and Plaintiffs and the Classes.

175. Defendant was also subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Classes.

176. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Classes was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

177. Plaintiffs and the Classes were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in

collecting and storing the PII and PHI of Plaintiff and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting or redacting PII and PHI stored on Defendant's systems.

178. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Classes. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions to not comply with industry standards for the safekeeping of the PII and PHI of Plaintiffs and the Classes, including basic encryption techniques freely available to Defendant.

179. Plaintiffs and the Classes had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

180. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

181. Defendant had and continues to have a duty to adequately disclose that the PII and PHI of Plaintiffs and the Classes within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

182. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiffs and the Classes.

183. Defendant has admitted that the PII and PHI of Plaintiffs and the Classes was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

184. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Classes by failing to implement industry standard protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiffs and the Classes during the time the PII and PHI was within Defendant's possession or control.

185. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiffs and the Classes in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

186. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiffs and the Classes in the face of increased risk of theft.

187. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Classes by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former patients', employees', and physicians' PII and PHI.

188. Defendant, through their actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Classes the existence and scope of the Data Breach.

189. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Classes, the PII and PHI of Plaintiffs and the Classes would not have been compromised.

190. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiffs and the Classes and the present harm, or risk of imminent harm, suffered by Plaintiffs and the Classes. The PII and PHI of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

191. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

192. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Classes.

193. With respect to Plaintiff Franchi and the Patient Class, Defendant violated Title II of HIPAA and regulations implemented by the HHS pursuant to HIPAA, as well as the standards of conduct established by HIPAA and its attendant regulations, which required Defendant to implement security measures to protect PHI.

194. Defendant's violation of Section 5 of the FTC Act and Title II of HIPAA, including HIPAA regulations HHS has implemented pursuant to Title II, as well as the standards of conduct established by these statutes and regulations, constitutes negligence per se.

195. Plaintiffs and the Classes are within the class of persons that the FTC Act was intended to protect.

196. Plaintiff Franchi and the Patient Class are within the class of persons that the HIPAA was intended to protect.

197. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Classes.

198. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs and the Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII and PHI of Plaintiffs and the Classes; and (viii) costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Classes.

199. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs and the Classes have suffered and will continue to suffer other forms of injury and/or harm,

including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

200. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiffs and the Classes have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

201. Plaintiffs and Class Members are therefore entitled to damages, including actual and compensatory damages, restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

**SECOND CAUSE OF ACTION**
**INVASION OF PRIVACY**
**At Common Law**
**(On Behalf of Plaintiffs and the Class)**

202. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

203. Plaintiffs bring this Count on their own behalf and on behalf of the Class.

204. The State of California recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

205. Plaintiffs and the Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

206. Defendant owed a duty to its current and former employees and physicians, including Plaintiff and the Class, to keep their Private Information contained as a part thereof, confidential.

207. Defendant failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiffs and the Class.

208. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and the Class, by way of Defendant's failure to protect the PII and PHI.

209. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and the Class is highly offensive to a reasonable person.

210. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class disclosed their Private Information to Defendant as part of their medical care or employment with Defendant, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

211. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

212. Defendant acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that its information security practices were inadequate and insufficient.

213. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class.

214. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiffs and the Class was disclosed to third parties without authorization, causing Plaintiffs and the Class to suffer damages.

215. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

**THIRD CAUSE OF ACTION**
**INVASION OF PRIVACY**
**Cal. Const. ART. 1 § 1**
**(On Behalf of Plaintiffs and the California Class)**

216. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

217. Plaintiffs bring this Count on their own behalf and on behalf of the California Class (the "Class" for the purposes of this Count).

218. California established the right to privacy in Article I, Section 1 of the California Constitution.

219. Plaintiffs and the Class had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

220. Defendant owed a duty to its current and former employees, physicians, and patients, including Plaintiffs and the Class, to keep their Private Information contained as a part thereof, confidential.

221. Defendant failed to protect and released to unknown and unauthorized third parties the PII and PHI of Plaintiffs and the Class.

222. Defendant allowed unauthorized and unknown third parties access to and examination of the Private Information of Plaintiffs and the Class, by way of Defendant's failure to protect the PII and PHI.

223. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and the Class is highly offensive to a reasonable person.

224. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Class disclosed their Private Information to Defendant as part of their medical care or employment with Defendant, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

225. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

226. Defendant acted with a knowing state of mind when they permitted the Data Breach to occur because they were with actual knowledge that its information security practices were inadequate and insufficient.

227. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Class.

228. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiffs and the Class was disclosed to third parties without authorization, causing Plaintiffs and the Class to suffer damages.

229. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

## FOURTH CAUSE OF ACTION
## BREACH OF IMPLIED CONTRACT
**(On Behalf of Plaintiffs and the Class, the Employee Class, and Patient Class)**

230. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

231. Plaintiffs bring this Count on their own behalf and on behalf of the Class, the Employee Class, and the Patient Class (the "Classes" for the purposes of this Count).

232. Plaintiffs and the Class Members delivered their Private Information to Defendant as part of the process of obtaining services or employment provided by Defendant.

233. 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 if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiffs' and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

234. In providing their Private Information, Plaintiffs and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Private Information.

235. In delivering their Private Information to Defendant, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard that data.

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

237. Defendant accepted possession of Plaintiffs' and Class Members' personal data for the purpose of providing medical services or employment to Plaintiffs and Class Members.

238. Had Defendant disclosed to Plaintiffs and Class Members that Defendant did not have adequate computer systems and security practices to secure patients' Private Information, Plaintiffs and members of the Classes would not have provided their Private Information to Defendant.

239. Defendant recognized that its current and former patients', employees', and physicians' 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 Class Members.

240. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

241. Defendant breached the implied contract with Plaintiffs and Class Members by failing to take reasonable measures to safeguard their data.

242. Defendant breached the implied contract with Plaintiffs and Class Members by failing to promptly notify them of the access to and exfiltration of their Private Information.

243. As a direct and proximate result of the breach of the contractual duties, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' Private Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Private Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiffs and the proposed classes entrusted Defendant with their Private Information; and (h) the continued and substantial risk to Plaintiffs' and Class Members' Private Information, which remains in the Defendant's possession of Defendant with inadequate measures to protect Plaintiffs' and Class Members' Private Information.

## FIFTH CAUSE OF ACTION
## CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT
## Cal. Civ. Code § 56, *et seq*.
## (On Behalf of Plaintiff Franchi and the Patient Class)

244. Plaintiff Franchi re-alleges and incorporates by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

245. Plaintiff Franchi ("Plaintiff" for the purposes of this Count) brings this Count on this own behalf and on behalf of the Patient Class (the "Class" for the purposes of this Count).

246. Defendant is "a provider of health care," as defined in Cal. Civ. Code §56.05(m), and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

247. At all relevant times, Defendant was a health care provider because they had the "purpose of maintaining medical information to make the information available to the individual or to a provider

of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manager his or her information, or for the diagnosis or treatment of the individual."

248. As a provider of health care or a contractor, Defendant is required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated or released without patient's authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

249. As a provider of health care or a contractor, Defendant is required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104.

250. Defendant is a person licensed under California under California's Business and Professions Code, Division 2. *See* Cal. Bus. Prof. Code § 4000, *et seq.*

251. Plaintiff and Class Members are "patients" as defined in CMIA, Cal. Civ. Code §56.05(k) ("'Patient' means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains."). Furthermore, Plaintiff and Class Members, as patients and customers of Defendant, 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, and were patients on or before the date of the Data Breach.

252. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Defendant's employees, which allowed the hackers to see and obtain Plaintiff's and Class Members' medical information.

253. Defendant negligently created, maintained, preserved, stored, and then exposed Plaintiff's and Class Members' individually identifiable "medical information," within the meaning of Cal. Civ. Code § 56.05(j), including Plaintiff's and Class Members' names, addresses, medical information, and health insurance information, that alone or in combination with other publicly available information, reveals their identities. Specifically, Defendant knowingly allowed and affirmatively acted in a manner

that allowed unauthorized parties to access and actually view Plaintiff's and Class Members' confidential Private Information.

254. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff and Class Members to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and Class Members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

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

256. Plaintiff's and Class Members' medical information was accessed, removed and actually viewed by hackers and other unauthorized parties during and following the Data Breach.

257. Plaintiff's and Class Members' medical information that was the subject of the Data Breach 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).

258. Defendant's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A). As a direct and proximate result of Defendant's above-noted wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia,

a. present, imminent, immediate and 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,

b. invasion of privacy,

c. breach of the confidentiality of the PHI,

d. statutory damages under the California CMIA,

e. deprivation of the value of their PHI, for which there is well-established national and international markets, and/or,

f. the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

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

260. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff's and Class Members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA.

261. Plaintiff's and the Class Members were injured and have suffered damages, as described above, from Defendant's illegal and unauthorized disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, which allows for actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

## SIXTH CAUSE OF ACTION
## VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
## Cal. Civ. Code § 1798, *et seq.*
## (On behalf of Plaintiff Aragon and the California Class)

262. Plaintiff Aragon re-allege and incorporate by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

263. Plaintiff Aragon brings this Count on his own behalf and on behalf of the California Class (the "Class" for the purposes of this Count).

264. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from

unauthorized access and disclosure. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[47]

265. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

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

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

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

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

---

[47] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

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

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

c. does business in California; and

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

270. The Private Information taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiffs' and the Class Members' unencrypted first and last names and Social Security numbers among other information.

271. Plaintiff Aragon and the California Class's Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their Private Information, including name and contact information was wrongfully taken, accessed, and viewed by unauthorized third parties.

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

273. On August 26, 2022, Plaintiff Aragon provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). If Defendant fails to respond or has

not cured or is unable to cure the violation within 30 days thereof, Plaintiff will amend this Complaint to seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. See Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

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

**SEVENTH CAUSE OF ACTION**
**CALIFORNIA UNFAIR COMPETITION LAW**
**Cal. Bus. & Prof. Code § 17200, *et seq*.**
**(On Behalf of Plaintiffs and the Class)**

275. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

276. Plaintiffs bring this Count on their own behalf and on behalf of the Class.

277. Defendant's acts and omissions as alleged herein emanated and directed from California.

278. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

279. Defendant stored the Private Information of Plaintiffs and Class Members in its computer systems.

280. Defendant knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiffs' and Class Members' PII secure and prevented the loss or misuse of that Private Information.

281. Defendant did not disclose at any time that Plaintiffs' and Class Members' Private Information was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only one in possession of that material information, which Defendant had a duty to disclose.

**Unlawful Business Practices**

282. As noted above, Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, by omission, the safety of their computer systems, specifically the security thereof, and its ability to safely store Plaintiffs' and California Subclass Members' Private Information.

283. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security.

284. If Defendant had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiffs and Class Members of the Data Breach.

285. Defendant's acts and omissions as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the FTC Act.

286. Defendant also violated the CMIA, as described above.

287. Plaintiffs and Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, Plaintiffs' and Class Members' Private Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

**Unfair Business Practices**

288. Defendant engaged in unfair business practices under the "balancing test." The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and failure to disclose inadequacies of Defendant's data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiffs and Class Members, directly causing the harms alleged below.

289. Defendant engaged in unfair business practices under the "tethering test." Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

290. Defendant engaged in unfair business practices under the "FTC test." The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects thousands of Class Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiffs' and Class Members' Private Information to third parties without their consent, diminution in value of their Private Information, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiffs' and Class Members' PII remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. See 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g., In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

291. Plaintiffs and Class Members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. Plaintiffs' and Class Members' Private Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value,

making it clear that the hacked information is of tangible value. Plaintiffs and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

292. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, Plaintiffs and Class Members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

## EIGHTH CAUSE OF ACTION
## DECLARATORY JUDGMENT
**(On Behalf of Plaintiffs and the Class, the Employee Class, and Patient Class)**

293. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in the preceding paragraphs as though fully set forth herein.

294. Plaintiffs bring this Count on their own behalf and on behalf of the Class, the Employee Class, and the Patient Class (the "Classes" for the purposes of this Count).

295. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

296. Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the Private Information it collected from Plaintiffs and Class Members.

297. Defendant owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure PII.

298. Defendant still possesses PII and PHI regarding Plaintiffs and Class Members.

299. Since the Data Breach, Defendant has announced few if any specific and significant changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

300. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the Private Information in Defendant's possession is even more vulnerable to cyberattack.

301. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further,

Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PII and PHI and Defendant's failure to address the security failings that lead to such exposure.

302. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

303. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

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

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

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

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

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

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

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

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

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiffs, on behalf of themselves and the members of the Classes, request judgment against Defendant and that the Court grant the following:

A. For an order certifying the Classes, as defined herein, and appointing Plaintiffs and their Counsel to represent each such 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 the members of the Classes, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and the members of the Classes;

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 the members of the Classes, 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 personal identifying information of Plaintiffs and the members of the Classes 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 the members of the Classes;

///

///

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 the members of the Classes;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and the members of the Classes 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 personal identifying information, as well as protecting the personal identifying information of Plaintiff 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 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 members of the Classes about the threats that they face as a result of the loss of their confidential Private 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. Ordering Defendant to pay for a lifetime of credit monitoring services for Plaintiffs and the Class;

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

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

G. For prejudgment and/or post-judgment interest on all amounts awarded; and

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

///

///

## DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

DATED: September 15, 2022

Respectfully Submitted,

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

Bryan L. Bleichner (SBN 220340)
**CHESTNUT CAMBRONNE PA**
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Email: *bbleichner@chesnutcambronne.com*

Dylan J. Gould (*pro hac vice* forthcoming)
**MARKOVITS, STOCK & DEMARCO, LLC**
119 E. Court St., Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Email: *dgould@msdlegal.com*

Gary M. Klinger (*pro hac vice* forthcoming)
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
227 W. Monroe Street, Ste. 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Email: *gklinger@milberg.com*

Jean S. Martin*
Francesca Kester*
**MORGAN & MORGAN COMPLEX LITIGATION GROUP**
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Email: *jeanmartin@forthepeople.com*
Email: *fkester@forthepeople.com*

*Attorneys for Plaintiff and the Proposed Class*

**PROOF OF SERVICE**

I, Lori Martin, declare and state:

I am a citizen of the United States, over 18 years of age, employed in the county of Sacramento, and not a party to the within action. My business address is 865 Howe Avenue, Sacramento, CA 95825.

On the date set forth below, I served the following on the parties in said action by the means indicated below:

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

1. **NEGLIGENCE;**
2. **COMMON LAW INVASION OF PRIVACY;**
3. **CAL. CONST. ART. 1 § 1 INVASION OF PRIVACY**
4. **BREACH OF IMPLIED CONTRACT**
5. **CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CAL. CIV. CODE § 56, *et seq*.;**
6. **CALIFORNIA CONSUMER PRIVACY ACT;**
7. **CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200, *et seq*.AND**
8. **DECLARATORY RELIEF.**

**DEMAND FOR JURY TRIAL**

[X] (BY TRANSMITTING VIA EMAIL OR ELECTRONIC TRANSMISSION) the document(s) listed above to the addressees listed below at the email addresses indicated, from lori@justice4you.com:

| | |
|---|---|
| Bryan L. Bleichner (SBN 220340)<br>**CHESTNUT CAMBRONNE PA**<br>100 Washington Avenue South, Suite 1700<br>Minneapolis, MN 55401<br>Phone: (612) 339-7300<br>Email: *bbleichner@chesnutcambronne.com*<br><br>*Attorneys for Plaintiff and the Proposed Class* | Dylan J. Gould (*pro hac vice* forthcoming)<br>**MARKOVITS, STOCK & DEMARCO, LLC**<br>119 E. Court St., Suite 530<br>Cincinnati, OH 45202<br>Phone: (513) 651-3700<br>Fax: (513) 665-0219<br>Email: *dgould@msdlegal.com*<br><br>*Attorneys for Plaintiff and the Proposed Class* |

| | |
|---|---|
| Gary M. Klinger (*pro hac vice* forthcoming)<br>**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**<br>227 W. Monroe Street, Ste. 2100<br>Chicago, IL 60606<br>Telephone: (866) 252-0878<br>Email: *gklinger@milberg.com*<br><br>*Attorneys for Plaintiff and the Proposed Class* | Jean S. Martin*<br>Francesca Kester*<br>**MORGAN & MORGAN COMPLEX LITIGATION GROUP**<br>201 N. Franklin Street, 7th Floor<br>Tampa, Florida 33602<br>Telephone: (813) 223-5505<br>Email: *jeanmartin@forthepeople.com*<br>Email: *fkester@forthepeople.com*<br><br>*Attorneys for Plaintiff and the Proposed Class* |
| Alexis B. Cruz, Esq.<br>Bethany G. Lukitsch, Esq.<br>Baker & Hostetler LLP<br>11601 Wilshire Boulevard, Suite 1400<br>Los Angeles, CA 90025-1744<br>Phone: 310-820-8800<br>Fax: 310-820-8859<br>Email: *acruz@bakerlaw.com; blukitsch@bakerlaw.com*<br><br>*Attorneys for Defendant* | |

I declare under penalty of perjury under the laws of the state of California that the foregoing is true and correct. Executed on September 15, 2022, at Sacramento, California.

/s/ Lori Martin
Lori Martin