Jonathan M. Rotter (SBN 234137)
Pavithra Rajesh (SBN 323055)
GLANCY PRONGAY & MURRAY LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
jrotter@glancylaw.com
prajesh@glancylaw.com

Daniel O. Herrera (*pro hac vice* anticipated)
Nickolas J. Hagman (*pro hac vice* anticipated)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Attorneys for Plaintiffs and the Proposed Class

[Additional Counsel on Signature Page]

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

SHANNON MASSER DOWNS, M.B., a minor, by and through her legal guardian, Shannon Masser Downs, and MARIA HINESTROSA, individually, and on behalf of all others similarly situated, Plaintiffs, v. REGAL MEDICAL GROUP, INC., LAKESIDE MEDICAL ORGANIZATION, A MEDICAL GROUP, INC., AFFILIATED DOCTORS OF ORANGE COUNTY MEDICAL GROUP, INC., and GREATER COVINA MEDICAL GROUP, INC. Defendants.	Case No. _____ **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Shannon Masser Downs, and M.B., a minor, by and through her legal guardian Shannon Masser Downs, and Maria Hinestrosa (collectively, "Plaintiffs"), individually, and on behalf of all others similarly situated, bring this action against Regal Medical Group, Inc., Lakeside Medical Organization, A Medical Group, Inc., Affiliated Doctors of Orange County Medical Group, Inc., and Greater Covina Medical Group, Inc., (collectively, "Regal" or "Defendants"), by and through their attorneys, and allege, based upon personal knowledge as to their own actions, and based upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Defendants are full-service medical groups providing healthcare services through its network of medical groups in Southern California.[1]

2. As one of the largest physician-led healthcare networks in Southern California, Defendants contract with doctors, hospitals, and urgent care centers to provide patients with options for managing their health.[2]

3. In doing so, Defendants collect, maintain, and store their patients' highly sensitive personal and medical information including, but not limited to: Social Security numbers, dates of birth, full names, addresses, telephone numbers, information regarding medical treatment and diagnosis, prescription data, laboratory test results, radiology reports, health plan member numbers, and other protected

[1] *See About Us*, Regal Medical Group, https://www.regalmed.com/about-us/ (last accessed Feb. 22, 2023); *About Us*, Lakeside Community Healthcare, https://www.lakesidemed.com/about-us/ (last accessed Feb. 22, 2023); *About Us*, ADOC Medical Group, https://www.adoc.us/about-us/ (last accessed Feb. 22, 2023); *About Us*, Greater Covina Medical Group Inc., https://www.gcmg.org/about-us/ (last accessed Feb. 22, 2023).

[2] *About Us*, Regal Medical Group, https://www.regalmed.com/about-us/ (last accessed Feb. 22, 2023).

health information ("personally identifying information" or "PII").[3]

4. Although Defendants are sophisticated medical entities providing services to hundreds of thousands of patients, Defendants failed to invest in adequate data security, thereby allowing hackers to exfiltrate the highly-sensitive personal and medical information of approximately 3,300,638 individuals, including the Plaintiffs and Class members.[4] As a direct, proximate, and foreseeable result of Defendants' failure to implement reasonable security protections sufficient to prevent an eminently avoidable cyberattack, unauthorized actors compromised Defendants' network and accessed millions of patient files containing highly-sensitive PII.[5]

5. Specifically, began on or around December 1, 2022, Defendants' patients' sensitive personal and medical data was compromised when unauthorized actors were able to breach Defendants' network and access files containing approximately 3,300,638 individual's PII (the "Data Breach").[6]

---

[3] *Submitted Breach Notification Sample*, Office of the Attorney General California Department of Justice, https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf (last accessed Feb. 22, 2023).

[4] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (las accessed Feb. 22, 2023); *see 3.3 Million Impacted by Ransomware Attack at California Healthcare Provider*, Security Week, https://www.securityweek.com/3-3-million-impacted-by-ransomware-attack-at-california-healthcare-provider/ (last accessed Feb. 22, 2023).

[5] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (las accessed Feb. 22, 2023); *see 3.3 Million Impacted by Ransomware Attack at California Healthcare Provider*, Security Week, https://www.securityweek.com/3-3-million-impacted-by-ransomware-attack-at-california-healthcare-provider/ (last accessed Feb. 22, 2023).

[6] *Submitted Breach Notification Sample*, Office of the Attorney General California Department of Justice,

6. Despite the fact that many of the categories of PII exposed in the Data Breach, such as Social Security numbers and medical information, cannot be changed, Defendants failed to detect the breach until a week later, on or around December 8, 2022, and failed to notify affected individuals until on or around February 1, 2023—approximately two months after unauthorized individuals accessed Plaintiffs' and current and former patients' highly sensitive PII stored on Defendants' systems.[7]

7. Defendants' failure to promptly notify Plaintiffs and Class members that their PII was exfiltrated due to Defendants' security failures virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse and/or disseminate that PII before Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

8. Defendants failed to take sufficient and reasonable measures to safeguard their data security systems and protect highly sensitive data in order to prevent the Data Breach from occurring; to disclose to current and former patients the material fact that it lacked appropriate data systems and security practices to secure PII and medical information; and to timely detect and provide adequate notice of the Data Breach to affected individuals. Due to Defendants' failures, Plaintiffs and approximately 3,300,638 individuals suffered substantial harm and injury.

---

https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf (last accessed Feb. 22, 2023); *see Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (las accessed Feb. 22, 2023).

[7] *Submitted Breach Notification Sample*, Office of the Attorney General California Department of Justice, https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf (last accessed Feb. 22, 2023).

9. As a result of Defendants' negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiffs' and Class members' PII was accessed and acquired by unauthorized third-parties for the express purpose of misusing the data and causing further irreparable harm to the personal, financial, reputational, and future well-being of Defendants' current and former patients. Plaintiffs and Class members face the real, immediate, and likely danger of identity theft and misuse of their PII, especially because their PII was specifically targeted by malevolent actors.

10. Plaintiffs and Class members suffered injuries as a result of Defendants' conduct including, but not limited to: lost or diminished value of their PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; time needed to change usernames and passwords on their accounts; time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach; charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their PII. These risks will remain for the lifetimes of Plaintiffs and the Class.

11. Accordingly, Plaintiffs bring this action on behalf of all those similarly situated to seek relief from Defendants' failure to reasonably safeguard Plaintiffs' and Class members' PII; their failure to reasonably provide timely notification that Plaintiffs' and Class members' PII had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiffs and Class

members concerning the status, safety, location, access, and protection of their PII.

PARTIES

Plaintiffs Shannon Masser Downs and M.B.

12. Plaintiff Shannon Masser Downs is a resident and citizen of California, residing in Valencia, California. Plaintiff Shannon Downs received from Defendants a letter concerning the data breach dated February 1, 2023.

13. Plaintiff M.B., a minor, is a resident and citizen of California, residing in Valencia, California. Plaintiff M.B. received from Defendants a letter concerning the data breach dated February 1, 2023.

Plaintiff Maria Hinestrosa

14. Plaintiff Hinestrosa is a resident and citizen of California, residing in Los Angeles, California. Plaintiff Hinestrosa received a data breach letter from Defendants that was dated February 1, 2023.

Defendant Regal Medical Group, Inc.

15. Defendant Regal Medical Group, Inc. is a healthcare network connecting patients to doctors, hospitals, and urgent care centers organized under the laws of the State of California with its principal place of business at 3115 Ocean Front Walk, 301, Marina Del Rey, CA, 90292.

Defendant Lakeside Medical Organization, A Medical Group, Inc.

16. Defendant Lakeside Medical Organization, A Medical Group, Inc. is a healthcare network connecting patients to doctors, hospitals, and urgent care centers organized under the laws of the State of California with its principal place of business at 3115 Ocean Front Walk, 301, Marina Del Rey, CA, 90292.

Defendant Affiliated Doctors of Orange County Medical Group, Inc.

17. Defendant Affiliated Doctors of Orange County Medical Group, Inc. is a healthcare network connecting patients to doctors, hospitals, and urgent care centers organized under the laws of the State of California with its principal place of business at 3115 Ocean Front Walk, 301, Marina Del Rey, CA, 90292.

Defendant Greater Covina Medical Group, Inc.

18. Defendant Greater Covina Medical Group, Inc. is a practice association with a healthcare network connecting patients to doctors and specialists organized under the laws of the State of California with its principal place of business at 605 East Badillo Street, 300, Covina, CA, 91723.

JURISDICTION AND VENUE

19. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at least one member of the Class is a citizen of a state different from Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

20. This Court has personal jurisdiction over Defendants because Defendants are authorized to and regularly conduct business in California, and is headquartered in this District.

21. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiffs' and Class members' claims occurred in this District.

FACTUAL ALLEGATIONS

A. Defendants – Background

22. Defendants are affiliated full-service medical groups that provide a variety of health care services including medical services and treatment from primary care physicians, specialists, hospitals, urgent care centers and labs and care resources including exercise programs, cooking classes, condition management programs and

individual coaching.[8] Defendants represent to their patients that they will "help organize and coordinate all of your care, and provide valuable health programs and services."[9]

23. As part of their medical and business operations, Defendants collect, maintain, and store the highly sensitive PII and medical information provided by their current and former patients, including but not limited to: Social Security numbers, dates of birth, full names, addresses, telephone numbers, information regarding medical treatment and diagnosis, prescription data, laboratory test results, radiology reports, and health plan member numbers.

24. On information and belief, at the time of the Data Breach, Defendants failed to implement necessary data security safeguards, which resulted in unauthorized third parties accessing the PII of approximately 3,300,608 current and former patients.[10]

25. Current and former patients of Defendants, such as Plaintiffs and Class members, allowed their PII to be made available to Defendants with the reasonable expectation that Defendants would comply with its obligation to keep their sensitive and personal information, including their PII, confidential and secure from illegal and unauthorized access, and that Defendants would provide them with prompt and accurate notice of any unauthorized access to their PII.

26. Unfortunately for Plaintiffs and Class members, Defendants failed to

[8] *About Us*, Regal Medical Group, https://www.regalmed.com/about-us/ (last accessed Feb. 22, 2023).

[9] *About Us*, Regal Medical Group, https://www.regalmed.com/about-us/ (last accessed Feb. 22, 2023).

[10] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Feb. 22, 2023).

carry out their duty to safeguard sensitive PII and provide adequate data security, thus failing to protect Plaintiffs and Class members from the exfiltration of their PII during the Data Breach.

B. The Data Breach

27. Defendants disclosed in a Notice sent on or about February 1, 2023, to Plaintiffs and other affected individuals that they were affected by a "ransomware cyberattack" in which an unauthorized third party accessed Defendants' servers, installed malware on some of Defendants' servers, and exfiltrated data concerning Defendants' current and former patients. *See* Notice of Data Breach, attached hereto as **Exhibit A**. Further, Defendants acknowledge that the unauthorized actor was able to exfiltrate Plaintiffs' and Class members' PII, Social Security numbers, and medical information.

28. Defendants further admitted that employees began experiencing "difficulty in accessing some of [Defendants'] servers" on December 2, 2022. *See id.* Despite experiencing the effects of the Data Breach on or about December 2, 2022, Defendants did not discovery the Data Breach until December 8, 2022. *Id.*

29. Defendants failed to disclose to Plaintiffs and other victims of the Data Breach when the unauthorized third party first gained access to Defendants' systems and how long the unauthorized actor had access to Plaintiffs' and Class members' information. Instead, Defendants admitted to the Office of the California Attorney General that the unauthorized actor(s) had unfettered access to Defendants' computer systems, and Plaintiffs' and other patients' PII, Social Security numbers, and other medical information.[11]

30. Defendants assert that upon discovering the Data Breach, it "worked

[11] *Submitted Breach Notification Sample*, Office of the Attorney General California Department of Justice, https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf (last accessed Feb. 22, 2023).

with [its] vendors to efficiently restore access to [its] systems and to analyze the impacted data." *See* Exhibit A. However, Defendants were not able to secure its computer systems until on or after December 8, 2022, seven days after the Data Breach occurred, and six days after first experiencing issues related to the Data Breach.[12] Defendants failed to disclose to Plaintiffs and Class members that Defendants were unable to quickly remove the hacker's access to Defendants' computer systems. *See* Exhibit A.

31. Despite discovering the Data Breach on December 8, 2022, and confirming that the unauthorized actor accessed and exfiltrated patients' PII, Social Security numbers, and medical records, Defendants delayed sending individualized notice to affected patients until on or after February 1, 2023. *See* Exhibit A.

32. During the time that the unauthorized individuals had unrestricted access to Defendants' network, they were able to access and acquire personal, sensitive, and protected PII and medical information belonging to over 3,300,608 current and former patients of Defendants.

C. Defendants' Many Failures Both Prior to and Following the Breach

33. Defendants could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and network files containing PII.

34. To be sure, collecting, maintaining, and protecting PII is vital to virtually every aspect of Defendants' operations as a medical group.

35. Despite such importance, Defendants failed to detect that their own data systems were compromised until on or around December 8, 2022.[13]

36. Moreover, when Defendants finally acknowledged that they had

[12] *Id.*

[13] *Submitted Breach Notification Sample*, Office of the Attorney General California Department of Justice, https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf (last accessed Feb. 22, 2023).

experienced a breach, they failed to fully inform affected individuals of the length of time that the unauthorized actors had access to their PII, or even the full extent of the PII that was accessed during the Data Breach.

37. Defendants' failure to properly safeguard Plaintiffs' and Class members' PII and medical information allowed the unauthorized actors to access this highly sensitive PII and medical information, and Defendants' failure to timely notify Plaintiffs and other victims of the Data Breach that their PII had been misappropriated precluded them from taking meaningful steps to safeguard their identities prior to the dissemination of their PII.

38. The Data Breach also highlights the inadequacies inherent in Defendants' network monitoring procedures. If Defendants had properly monitored their cyber security systems, they would have prevented the Data Breach, discovered the Data Breach sooner, and/or have prevented the hackers from exfiltrating PII and medical information.

39. Defendants' delayed response only further exacerbated the consequences of the Data Breach brought on by its systemic IT failures.

40. First, Defendants failed to timely secure their computer systems to protect their current and former patients' PII and medical information. Defendants allowed the unauthorized actors to continue to have unfettered access to Defendants' systems for seven days—six days after Defendants first began experiencing issues related to the Data Breach—until Defendants finally discovered the Data Breach.

41. Second, Defendants failed to timely notify affected individuals, including Plaintiffs and Class members, that their highly-sensitive PII had been accessed by unauthorized third parties. Defendants waited two months after discovering the Data Breach to provide notice to the victims of the Data Breach that their PII had been compromised.

42. Third, Defendants made no effort to protect Plaintiffs and the Class from the long-term consequences of Defendants' acts and omissions. Although the Notice

offered victims one-year of complimentary Norton LifeLock credit monitoring, Plaintiffs' and Class members' PII, including their Social Security numbers, cannot be changed and will remain at risk long beyond one year. As a result, Plaintiffs and the Class will remain at a heightened and unreasonable risk of identity theft for the remainder of their lives.

43. In short, Defendants' myriad failures, including the failure to timely detect the Data Breach and to notify Plaintiffs and Class members with reasonable timeliness that their personal and medical information had been exfiltrated due to Defendants' security failures, allowed unauthorized individuals to access and misappropriate Plaintiffs' and Class members' PII for months before Defendants finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

44. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

45. In 2018, the Identity Theft Resource Center and CyberScout Annual End-of-Year Data Breach Report revealed a 126% increase in exposed data.[14] Between January and July 2019, more than 31.6 million healthcare records were exposed in data security incidents—more than double the total amount of healthcare data breaches for all of 2018.[15]

[14] *2018 End of Year Data Breach Report*, Identity Theft Resource Center, available at https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf (last accessed July 20, 2022).

[15] Steve Adler, *First Half of 2019 Sees 31.6 Million Healthcare Records Breached*, HIPAA Journal (Aug. 2, 2019), available at: https://www.hipaajournal.com/first-half-of-2019-sees-31-million-healthcare-records-breached.

46. In fact, Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, estimates that the annual number of data breaches occurring in the United States increased by approximately 692% between 2005 and 2018, a year during which over 446.5 million personal records were exposed due to data breach incidents.[16] Conditions have only worsened since: Statista estimates that "[i]n 2019, the number of data breaches in the United States amounted to 1,473 with over 164.68 million sensitive records exposed[,]" and that "[i]n the first half of 2020, there were 540 reported data breaches."[17]

47. Data breaches are a constant threat because of the price that PII are sold for on the dark web. According to Experian, medical records sell on the dark web for prices that are hundreds or thousands of times the price of basic personal or financial information.[18] For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

48. Individuals are particularly concerned with protecting the privacy of their financial account information and social security numbers. Neal O'Farrell, a security and identity theft expert for Credit Sesame, calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers." There are long-term

[16] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2020*, Statista, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-unitedstates-by-number-of-breaches-and-records-exposed (last accessed July 20, 2022).

[17] *Id.*

[18] *See* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, Experian (Dec. 6, 2017), available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.

consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiffs and Class members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."

49. Data breaches involving medical and health information, like the one here at issue, amplify those risks considerably because of the access it provides to criminals.

50. When the PII includes medical information, the identity theft could extend to sending the victim fake medical bills or obtaining medical services using the victim's insurance or financial information, which can result in unknown, unpaid bills being sent to collections or using the victim's health insurance.[19]

51. Moreover, unlike victims of just credit card identity theft, victims of medical records data breaches cannot simply "reverse" fraudulent transactions.[20] As such, victims of data breaches in which hackers misappropriate highly sensitive patient PII often are unable to recover the losses they suffer as a result thereof, and must expend additional time and money to mitigate and protect themselves from further attempts at identity theft. One study found that the majority of medical identity theft victims had to pay an average of $13,500 to resolve issues stemming from the

[19] Medical Identity Theft, Federal Trade Commission (Jan. 2011), available at: https://www.bulkorder.ftc.gov/system/files/publications/bus75-medical-identity-theft-faq-health-care-health-plan.pdf.

[20] *See The $300 Billion Attack: The Revenue Risk and Human Impact of Healthcare Provider Cyber Security Inaction*, Accenture, available at: https://www.accenture.com/_acnmedia/PDF-54/Accenture-Health-Cybersecurity-300-Billion-at-Risk.pdf (last visited Feb. 12, 2021).

data breach, and only 10% of victims achieve a completely satisfactorily resolution.[21] Almost one-third of medical identity theft victims lost their health insurance as a result of the identity theft.[22]

52. As explained by Kunal Rupani, director of product management at Accellion, a private cloud solutions company, in the context of a different medical data breach:

> Unlike credit card numbers and other financial data, healthcare information doesn't have an expiration date. As a result, a patient's records can sell on the black market for upwards of fifty times the amount of their credit card number, making hospitals and other healthcare organizations extremely lucrative targets for cybercriminals.[23]

53. SecureWorks, a division of Dell Inc., echoed that sentiment, noting that "[i]t's a well known truism within much of the healthcare data security community that an individual healthcare record is worth more on the black market ($50, on average) than a U.S.-based credit card and personal identity with social security number combined."[24] The reason is that thieves "[c]an use a healthcare record to submit false medical claims (and thus obtain free medical care), purchase prescription

---

[21] *See Fifth Annual Study on Medical Identity Theft*, Ponemon Institute LLC (Feb. 2015), at pp.2, 7, available at: https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65.

[22] *Id.*

[23] Jeff Goldman, 21st Century Oncology Notifies 2.2 Million Patients of Data Breach (Mar. 11, 2016), http://www.esecurityplanet.com/network-security/21st-century-oncology-notifies-2.2-million-patients-of-data-breach.html (last visited Feb. 11, 2021).

[24] What's the Market Value of a Healthcare Record, Dell SecureWorks (Dec. 13, 2012), https://www.secureworks.com/blog/general-market-value-of-a-healthcare-record (last visited Feb. 11, 2021).

medication, or resell the record on the black market."[25]

54. Similarly, the FBI Cyber Division in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.[26]

55. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Defendants that are charged with maintaining and securing patient PII know the importance of protecting that information from unauthorized disclosure. Indeed, on information and belief, Defendants were aware of highly publicized security breaches where PII and protected health information was accessed by unauthorized cybercriminals, including breaches of computer systems involving: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[27]

56. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International,

---

[25] *Id.*

[26] Federal Bureau of Investigation, FBI Cyber Division Private Industry Notification (Apr. 8, 2014), https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf (last visited Feb. 11, 2021).

[27] *See e.g.*, *Healthcare Data Breach Statistics*, HIPAA Journal, available at: https://www.hipaajournal.com/healthcare-data-breach-statistics (last accessed Feb. 15, 2021).

Inc., and others. The FTC publicized these enforcement actions to place companies like Defendants on notice of their obligation to safeguard customer and patient information.

57. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

58. Further, consumers' PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[28] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[29]

59. Social Security numbers are among the most dangerous kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

---

[28] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 20, 2022).

[29] Zachary Ignoffo, *Dark Web Price Index 2021*, PRIVACY AFFAIRS (Dec. 10, 2021), available at https://www.privacyaffairs.com/dark-web-price-index-2021/.

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[30]

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

61. 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."[31]

62. 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

[30] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION (July 2021), available at https://www.ssa.gov/pubs/EN-05-10064.pdf.

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

Security Numbers are worth more than 10x on the black market."[32]

63. Given the nature of Defendants' Data Breach, as well as the long delay in notification to the Class, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class members' PII can easily obtain Plaintiffs' and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

64. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[33] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

65. To date, Defendants has offered its consumers *only one year* of identity monitoring services. The offered services are inadequate to protect Plaintiffs and the Class from the threats they face for years to come, particularly in light of the PII at issue here.

66. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep PII private and secure, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and the Class from misappropriation. As a result, the injuries to Plaintiffs and the Class were directly and

---

[32] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, COMPUTER WORLD (Feb. 6, 2015), available at http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

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

proximately caused by Defendants' failure to implement or maintain adequate data security measures for its current and former patients.

E. Defendants Had a Duty and Obligation to Protect PII

67. Defendants has an obligation, both statutory and self-imposed, to keep confidential and protect from unauthorized access and/or disclosure Plaintiffs' and Class members' PII. Defendants' obligations are derived from: 1) government regulations and state laws, including HIPAA and FTC rules and regulations; 2) industry standards; and 3) promises and representations regarding the handling of sensitive PII and medical records. Plaintiffs and Class members provided, and Defendants obtained, their PII on the understanding that their PII would be protected and safeguarded from unauthorized access or disclosure.

68. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII, regularly review access to data bases containing protected information, and procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

69. Additionally, HIPAA requires Covered Entities and Business Associates to provide notification to every affected individual following the impermissible use or disclosures of any protected health information. The individual notice must be provided to affected individuals without unreasonable delay and no later than 60 days following discovery of the breach. Further, for a breach involving more than 500 individuals, entities are required to provide notice in prominent media outlets. *See* 45 CFR § 164.400, *et seq.*

70. Defendants represent to patients and customers that they will comply with HIPAA requirements concerning the protection of PII and protected health

information and prompt and adequate notification of data breaches.[34]

71. Additionally, the Federal Trade Commission's ("FTC") Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

72. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[35] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[36]

73. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-marking.[37]

74. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data

[34] *See, e.g.*, *Notice of Privacy Practices*, Regal Medical Group, https://www.regalmed.com/privacy-notice/ (last accessed Feb. 24, 2023).

[35] 17 C.F.R. § 248.201.

[36] *Id.*

[37] *Start With Security*, Federal Trade Commission (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

security principles and practices for business.[38] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[39] 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.[40] Defendants clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, and the amount of data exfiltrated.

75. Here, at all relevant times, Defendants were fully aware of their obligation to protect the PII and protected health information of their current and former patients, including Plaintiffs and the Class, and Defendants are sophisticated and technologically savvy medical treatment centers that rely extensively on technology systems and networks to maintain their medical practice, including transmitting their patients' PII, protected health information, and medical information in order to operate their business. [41]

---

[38] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (Jan. 23, 2015), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[39] *Id.*

[40] *Id.*

[41] *Submitted Breach Notification Sample*, Office of the Attorney General California Department of Justice, https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf (last accessed Feb. 22, 2023); *HIPAA Policies and Practices*, Regal Medical Group, https://www.regalmed.com/compliance-and-resources/hipaa-policies-and-procedures/ (last accessed Feb. 24, 2023).

76. Defendants had, and continue to have, a duty to exercise reasonable care in collecting, storing, and protecting the PII and medical information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendants, and Plaintiffs and Class members. Defendants alone had the exclusive ability to implement adequate security measures to their cyber security network to secure and protect Plaintiffs' and Class members' PII.

77. Defendants' failure to follow the FTC guidelines and their subsequent failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data constitutes unfair acts or practices prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 14 U.S.C. § 45.

78. Further, Defendants had a duty to promptly notify Plaintiffs and the Class that their PII was accessed by unauthorized persons.

F. Defendants Violated HIPAA, FTC and Industry Standard Data Protection Protocols

79. HIPAA obligates Covered Entities and Business Associates to adopt administrative, physical, and technology safeguards to ensure the confidentially, integrity, and security of consumer and patient PII.

80. The FTC rules, regulations, and guidelines obligate businesses to protect PII, from unauthorized access or disclosure by unauthorized persons.

81. At all relevant times, Defendants were fully aware of their obligation to protect the customers and patient PII because it is a sophisticated business entity that is in the business of maintaining and transmitting PII, including personal health and medical records.

82. Defendants were also aware of the significant consequences of their failure to protect PII for the hundreds of thousands of patients who provided their PII and medical information to Defendants, and knew that this data, if hacked, would injure consumers, including Plaintiffs and Class members.

83. Unfortunately, Defendants failed to comply with HIPAA, FTC rules,

regulations and guidelines, and industry standards concerning the protection and security of PII. As evidenced by the duration, scope, and nature of the Data Breach, among its many deficient practices, Defendants failed in, *inter alia*, the following respects:

a. Developing and employing adequate intrusion detection systems;
b. Engaging in regular reviews of audit logs and authentication records;
c. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;
d. Ensuring the confidentiality and integrity of current and former patients' PII, including protected health and information and records that Defendants receive and maintain;
e. Protecting against any reasonably anticipated threats or hazards to the security or integrity of its current and former patients' PII;
f. Implementing policies and procedures to prevent, detect, contain, and correct security violations;
g. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;
h. Implementing technical policies, procedures and safeguards for electronically stored information concerning PII that permit access for only those persons or programs that have specifically been granted access; and
i. Other similar measures to protect the security and confidentiality of its current and former patients' PII.

84. Had Defendants implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. Defendants could have prevented or detected the Data Breach prior to the hackers accessing Defendants' systems and extracting

sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and current and former patients of Defendants would have been notified sooner, allowing them to promptly take protective and mitigating actions.

G. Defendants' Data Security Practices are Inadequate and Inconsistent with its Self-Imposed Data Security Obligations

85. Defendants purport to care about data security and safeguarding patients' PII, and represents that they will keep secure and confidential the PII belonging to their current and former patients.

86. Plaintiffs' and Class members' PII and medical information was provided to Defendants in reliance on its promises and self-imposed obligations to keep PII and medical information confidential, and to secure the PII and medical information from unauthorized access by malevolent actors. Defendants failed to do so.

87. The length of the Data Breach also demonstrates that Defendants failed to safeguard PII by, *inter alia*: maintaining an adequate data security environment to reduce the risk of a data breach; periodically auditing its security systems to discover intrusions like the Data Breach; and retaining outside vendors to periodically test its network, servers, systems and workstations.

88. Had Defendants undertaken the actions that federal and state law require, the Data Breach could have been prevented or the consequences of the Data Breach significantly reduced, as Defendants would have detected the Data Breach prior to the hackers extracting data from Defendants' networks, and Defendants' current and former patients would have been notified of the Data Breach sooner, allowing them to take necessary protective or mitigating measures much earlier.

89. Indeed, following the Data Breach, Defendants effectively conceded that its security practices were inadequate and ineffective. In the Notice it sent to Plaintiffs and others, Defendants acknowledged that the Data Breach required it to "hire[] third-

party vendors experienced in this area to assist with our response to the incident" *See* Exhibit A.

H. Plaintiffs and the Class Suffered Harm Resulting from the Data Breach

90. Like any data hack, the Data Breach presents major problems for all affected. According to Jonathan Bowers, a fraud and data specialist at fraud prevention provider Trustev, "Give a fraudster your comprehensive personal information, they can steal your identity and take out lines of credit that destroy your finances for years to come."[42]

91. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[43]

92. The ramifications of Defendants' failure to properly secure PII, including Plaintiffs' and Class members' PII, are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission to commit fraud or other crimes.

93. According to data security experts, one out of every four data breach notification recipients becomes a victim of identity fraud.

94. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes

[42] Roger Cheng, *Data Breach Hits Roughly 15M T-Mobile Customers, Applicants*, CNET (Oct. 1, 2015), available at: http://www.cnet.com/news/data-breach-snags-data-from-15m-t-mobile-customers/. (last accessed July 20, 2022).

[43] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last accessed July 20, 2022).

time for an information breach to be detected.

95. Accordingly, Defendants' wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[44] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[45] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[46] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class members' PII will do so at a later date or re-sell it.

96. In response to the Data Breach, Defendants offered to provide certain individuals whose PII was exposed in the Data Breach with one year of credit monitoring. However, one year of complimentary credit monitoring is a time frame much shorter than what is necessary to protect against the lifelong risk of harm imposed on Plaintiffs and Class members by Defendants' failures.

97. Moreover, the credit monitoring offered by Defendants is inadequate to protect Plaintiffs and Class members from the injuries resulting from the unauthorized

---

[44] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), available at http://www.iii.org/insuranceindustryblog/?p=267.

[45] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), available at http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php.

[46] *The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas*, NORTHWESTERN UNIVERSITY, available at https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf.

access and exfiltration of their sensitive PII.

98. Here, due to the Breach, Plaintiffs and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of PII, including protected health information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the PII stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendants' delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their PII is exposed for theft and sale on the dark web; and

f. The loss of Plaintiffs' and Class members' privacy.

99. Plaintiffs and Class members have suffered imminent and impending

injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII and protected health information being accessed by cybercriminals, risks that will not abate within a mere one year: the unauthorized access of Plaintiffs' and Class members' PII, especially their Social Security numbers, puts Plaintiffs and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Defendants offered victims of the Breach. The one year of credit monitoring that Defendants offered to certain victims of the Data Breach is inadequate to mitigate the aforementioned injuries Plaintiffs and Class members have suffered and will continue to suffer as a result of the Data Breach.

100. As a direct and proximate result of Defendants' acts and omissions in failing to protect and secure PII and medical information, Plaintiffs and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

101. Plaintiffs retain an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose PII and medical information was accessed in the Data Breach.

102. Defendants are aware of the ongoing harm that the Data Breach has and will continue to impose on Defendants' current and former patients, as the notices that it posted and sent to Plaintiffs and Class members regarding the Data Breach advise the victims to "take immediate steps to protect themselves from potential harm[.]" *See* Exhibit A.

I. The Downs Plaintiffs' Experience

103. In February 2023, both Plaintiffs received notices from Defendants that each of their PII and medical treatment and health information had been improperly accessed and/or obtained by third parties. Each notice indicated that Plaintiffs' PII, inclusive of their Social Security numbers, dates of birth, full names, addresses, telephone numbers, information regarding medical treatment and diagnosis,

prescription data, laboratory test results, radiology reports, and health plan member numbers, were compromised in the Data Breach.

104. As a result of the Data Breach, Plaintiffs have 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 credit monitoring and identity theft protection services. Plaintiffs have spent several hours dealing with the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

105. Between December 2022 and February 2023, Plaintiff Shannon Masser Downs has received multiple notices that fraudulent activity is occurring within her authorized accounts. The notices included an alert that an unknown user attempted to register for a credit card in her name and that her Social Security Number had been breached.

106. As a result of the Data Breach, Plaintiffs have suffered anxiety as a result of the release of their PII, which they believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using their PII for purposes of identity theft and fraud. Plaintiffs are concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

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

108. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiffs are at a present

risk and will continue to be at increased risk of identity theft and fraud for years to come.

J. Plaintiff Hinestrosa's Experience

109. In February 2023, Plaintiff Hinestrosa received a notice from Defendants that her PII and medical information had been improperly accessed and/or obtained by third parties. This notice indicated that Plaintiff Hinestrosa's PII, inclusive of her Social Security number, date of birth, full name, address, telephone number, information regarding medical treatment and diagnosis, prescription data, laboratory test results, radiology reports, and health plan member number, were compromised in the Data Breach.

110. As a result of the Data Breach, Plaintiff Hinestrosa has 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 credit monitoring and identity theft protection services. Plaintiff Hinestrosa has spent several hours dealing with the Data Breach, valuable time Plaintiff Hinestrosa otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

111. In December of 2022, Plaintiff Hinestrosa received notice that an unauthorized actor had attempted to access her credit card. Additionally, in February of 2023, Plaintiff Hinestrosa received a notice from Citibank of fraudulent activity on her bank account, and, as a result, Citibank canceled her debit card and de-activated her account.

112. As a result of the Data Breach, Plaintiff Hinestrosa has suffered anxiety as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Hinestrosa is concerned about identity theft and fraud, as well as the consequences of

such identity theft and fraud resulting from the Data Breach.

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

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

CLASS ALLEGATIONS

115. Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All persons in the United States whose PII was accessed in the Data Breach.

Excluded from the Class are Defendants, their executives and officers, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change or expand the Class definition after conducting discovery.

116. In the alternative, Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

> All persons who are residents of the State of California whose PII was accessed in the Data Breach (the "California Subclass").

Excluded from the California Subclass are Defendants, their executives and officers, and the Judge(s) assigned to this case.

117. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in

the sole possession of Defendants and obtainable by Plaintiffs only through the discovery process, Plaintiffs believe, and on that basis allege, that approximately 3,300,638 individuals comprise the Class and were affected by the Data Breach. The members of the Class will be identifiable through information and records in Defendants' possession, custody, and control.

118. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether Defendants' data security and retention policies were unreasonable;

b. Whether Defendants failed to protect the confidential and highly sensitive information with which it was entrusted;

c. Whether Defendants owed a duty to Plaintiffs and Class members to safeguard their PII;

d. Whether Defendants breached any legal duties in connection with the Data Breach;

e. Whether Defendants' conduct was intentional, reckless, willful or negligent;

f. Whether an implied contract was created concerning the security of Plaintiffs' and Class members' PII;

g. Whether Defendants breached that implied contract by failing to protect and keep secure Plaintiffs' and Class members' PII and/or failing to timely and adequately notify Plaintiffs and Class members of the Data Breach;

h. Whether Plaintiffs and Class members suffered damages as a result of Defendants' conduct; and

i. Whether Plaintiffs and the Class are entitled to monetary damages,

injunctive relief and/or other remedies and, if so, the nature of any such relief.

119. Typicality: All of Plaintiffs' claims are typical of the claims of the Class since Plaintiffs and all members of the Class had their PII compromised in the Data Breach. Plaintiffs and the members of the Class sustained damages as a result of Defendants' uniform wrongful conduct.

120. Adequacy: Plaintiffs are adequate representatives because their interests do not materially or irreconcilably conflict with the interests of the Class they seek to represent, they have retained counsel competent and highly experienced in complex class action litigation, and intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Neither Plaintiffs nor their counsel have any interests that are antagonistic to the interests of other members of the Class.

121. Superiority: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendants records and databases.

122. Defendants have acted, and refused to act, on grounds generally

applicable to the Class, thereby making appropriate final relief with respect to the Class as a whole.

CAUSES OF ACTION

COUNT I –- Negligence
(By Plaintiffs on behalf of the Class, or, in the alternative, the California Subclass)

123. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

124. This count is brought on behalf of all Class members.

125. Defendants owed a duty to Plaintiffs and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the PII that Defendants collected.

126. Defendants owed a duty to Plaintiffs and the Class to provide security, consistent with industry standards and requirements, and to ensure that its cyber networks and systems, and the personnel responsible for them, adequately protected the PII that Defendants collected.

127. Defendants owed a duty to Plaintiffs and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it is discovered.

128. Defendants owed a duty of care to Plaintiffs and the Class because they were a foreseeable and probable victim of any inadequate data security practices.

129. Defendants solicited, gathered, and stored the PII belonging to Plaintiffs and the Class.

130. Defendants knew or should have known they inadequately safeguarded this information.

131. Defendants knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiffs and Class members, and Defendants were therefore charged with a duty to adequately protect this critically sensitive information.

132. Defendants had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' highly sensitive PII and medical information was entrusted to Defendants on the understanding that adequate security precautions would be taken to protect the PII and medical information. Moreover, only Defendants had the ability to protect its systems and the PII stored on them from attack.

133. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs, Class members, and their PII. Defendants' misconduct included failing to: (1) secure their systems, servers and networks, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the safeguards, policies, and procedures necessary to prevent this type of data breach.

134. Defendants breached their duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate cyber networks and data security practices to safeguard the PII belonging to Plaintiffs and the Class.

135. Defendants breached their duties to Plaintiffs and the Class by creating a foreseeable risk of harm through the misconduct previously described.

136. Defendants breached the duties they owed to Plaintiffs and Class members by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of PII.

137. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PII belonging to Plaintiffs and the Class so that Plaintiffs and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

138. Defendants breached the duties they owed to Plaintiffs and the Class by failing to disclose timely and accurately to Plaintiffs and Class members that their PII had been improperly acquired or accessed.

139. Defendants breached their duty to timely notify Plaintiffs and Class

members of the Data Breach by failing to provide direct notice to Plaintiffs and the Class concerning the Data Breach until on or about February 1, 2023.

140. As a direct and proximate result of Defendants' conduct, Plaintiffs and the Class have suffered a drastically increased risk of identity theft, relative to both the time period before the breach, as well as to the risk born by the general public, as well as other damages, including but not limited to time and expenses incurred in mitigating the effects of the Data Breach.

141. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II –- Negligence Per Se
(By Plaintiffs on behalf of the Class, or, in the alternative, the California Subclass)

142. Plaintiffs incorporate and realleges all allegations above as if fully set forth herein.

143. This count is brought on behalf of all Class members.

144. HIPAA obligates Covered Entities and Business Associates to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information" and "must reasonably safeguard protected health information." 45 CFR § 164.530(c).

145. In the event of a data breach, HIPAA obligates Covered Entities and Business Associates to notify affected individuals, prominent media outlets, and the Secretary of the Department of Health and Human Services of the data breach without unreasonable delay and in no event later than 60 days after discovery of the data breach. 45 CFR § 164.400, *et seq.*

146. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendants, of

failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

147. The California Customer Records Act ("CCRA"), Cal. Civ. Code § 1798.80, *et seq*., requires that entities in possession of PII take reasonable measures to protect the PII, and timely and fully disclose any breach of the security of the PII in the entity's possession.

148. Furthermore, the California Unfair Competition Law ("UCL") Cal. Bus. & Prof. Code §17200, *et seq.*, prohibits, inter alia, "any unlawful, unfair, or fraudulent business act or practice."

149. In addition to the FTC rules and regulations, the CCRA, and the UCL, other states and jurisdictions where victims of the Data Breach are located require that Defendants protect PII from unauthorized access and disclosure, and timely notify the victim of a data breach.

150. Defendants violated HIPAA, the CCRA, the UCL, and FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards, and by unduly delaying reasonable notice of the actual breach. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored, the foreseeable consequences of a Data Breach and the exposure of Plaintiffs' and Class members' sensitive PII.

151. Defendants' violations of HIPAA, the CCRA, the UCL, FTC rules and other applicable statutes, rules, and regulations constitutes negligence *per se*.

152. Plaintiffs and the Class are within the category of persons HIPAA, the CCRA, the UCL, and the FTC Act were intended to protect.

153. The harm that occurred as a result of the Data Breach described herein is the type of harm HIPAA, the CCRA, the UCL, and the FTC Act were intended to guard against.

154. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have been damaged as described herein, continue to suffer

injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendants' possession, and are entitled to damages in an amount to be proven at trial.

COUNT III –- Breach of Implied Contract
(By Plaintiffs on behalf of the Class, or, in the alternative, the California Subclass)

155. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

156. This count is brought on behalf of all Class members.

157. Plaintiffs and the Class provided Defendants with their PII and medical information.

158. By providing their PII and medical information, and upon Defendants' acceptance of such information, Plaintiffs and the Class, on one hand, and Defendants, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

159. The implied contracts between Defendants and Plaintiffs and Class members obligated Defendants to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiffs' and Class members' PII and medical information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. Defendants expressly adopted and assented to these terms in its public statements, representations and promises as described above.

160. The implied contracts for data security also obligated Defendants to provide Plaintiffs and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their PII and medical information.

161. Defendants breached the implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the PII and medical information belonging to Plaintiffs and Class members; allowing unauthorized persons to access Plaintiffs' and Class members' PII; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiffs and Class

members, as alleged above.

162. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiffs and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of their PII and medical information in Defendants possession, and are entitled to damages in an amount to be proven at trial.

COUNT IV –- Bailment
(By Plaintiffs on behalf of the Class, or, in the alternative, the California Subclass)

163. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

164. This count is brought on behalf of all Class members.

165. Plaintiffs' and Class members' PII was provided to Defendants.

166. In delivering their PII and, Plaintiffs and Class members intended and understood that their PII would be adequately safeguarded and protected.

167. Defendants accepted Plaintiffs' and Class members' PII.

168. By accepting possession of Plaintiffs' and Class members' PII, Defendants understood that Plaintiffs and the Class expected their PII to be adequately safeguarded and protected. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

169. During the bailment (or deposit), Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care, diligence, and prudence in protecting their PII.

170. Defendants breached their duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class members' PII, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and Class members' PII.

171. Defendants further breached their duty to safeguard Plaintiffs' and Class

members' PII by failing to timely notify them that their PII had been compromised as a result of the Data Breach.

172. Defendants failed to return, purge, or delete the PII belonging to Plaintiffs and Class members at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

173. As a direct and proximate result of Defendants' breach of their duties, Plaintiffs and the Class suffered consequential damages that were reasonably foreseeable to Defendants, including but not limited to the damages set forth herein.

174. As a direct and proximate result of Defendants' breach of their duty, Plaintiffs' and Class members PII that was entrusted to Defendants during the bailment (or deposit) was damaged and its value diminished.

COUNT V –- Violation of the California Unfair Competition Law
(By Plaintiffs on behalf of the Class, or, in the alternative, the California Subclass)

175. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

176. This count is brought on behalf of the California Subclass.

177. The California Unfair Competition Law ("UCL") Cal. Bus. & Prof. Code §17200, *et seq*., prohibits, inter alia, "any unlawful, unfair, or fraudulent business act or practice." Cal. Bus. & Prof. Code §17200.

178. Defendants engaged in unlawful, unfair, and fraudulent business acts or practices in violation of the UCL.

179. Defendants' acts, omissions, and conduct were "unlawful" because they violated the FTC Act and were negligent.

180. Defendants' acts, omissions, and conduct were also "unlawful" because they violated the California Customer Records Act ("CCRA"), Cal. Civ. Code § 1798.80, *et seq.* Defendants failed to take reasonable measures to protect Plaintiffs' and Class members' PII, in violation of Cal. Civ. Code § 1798.81.5. Defendants also

failed to timely and fully disclose the extent of the Data Breach in the Notice sent to Plaintiffs and Class members, in violation of Cal. Civ. Code § 1798.82.

181. Defendants' acts, omissions, and conduct were also "unlawful" because they violated the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), and the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code §56.10(a), by failing to implement proper procedures and filing to safeguard Plaintiffs' and Class members PII and confidential medical records.

182. Defendants' acts, omissions, and conduct were "unfair" because they offend public policy and constitute immoral, unethical, and unscrupulous activities that caused substantial injury, including to Plaintiffs and Class members. The gravity of harm resulting from Defendants' conduct outweighs any potential benefits attributable to the conduct and there were reasonably available alternatives to further Defendants' legitimate business interests. Defendants' unfair acts and practices include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including but not limited to duties imposed by HIPAA, the CCRA, the CCPA, the CMIA, and the FTC Act, which were direct and proximate causes of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and the Class members' PII;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Class members' PII;

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Class members' PII; and

h. Failing to promptly and adequately notify Plaintiffs and Class members that their PII was accessed by unauthorized persons in the Data Breach.

183. Defendants engaged in fraudulent business practices by making material misrepresentations and by failing to disclose material information regarding Defendants' deficient security policies and practices, the security of the PII of Plaintiffs and Class members, and the Data Breach.

184. Defendants had exclusive knowledge of material information regarding their deficient security policies and practices, and regarding the security of the PII of Plaintiffs and Class members. This exclusive knowledge includes, but is not limited to, information that Defendants received through internal and other non-public audits and that the PII of Plaintiffs and Class members was vulnerable.

185. Defendants also had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

186. Defendants also had exclusive knowledge about the length of time that

it maintained former patients' PII.

187. Defendants failed to disclose the material information it had regarding their deficient security policies and practices, and regarding the security of the PII of Plaintiffs and Class members. For example, even though Defendants have long known that its security policies and practices were substandard and deficient, and that the PII of Plaintiffs and Class members was vulnerable as a result, Defendants failed to disclose this information to Plaintiffs and Class members. Likewise, during the days and weeks following the Data Breach, Defendants failed to disclose information that it had regarding the extent and nature of the Data Breach.

188. Defendants had a duty to disclose the material information that they had because, *inter alia*, they had exclusive knowledge of the information, they actively concealed the information, and because Defendants were in a fiduciary position by virtue of the fact that Defendants collected and maintained Plaintiffs' and Class members' financial information, medical information, and other PII.

189. Defendants' representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendants' data security and its ability to protect the confidentiality of current and former employees' PII.

190. Had Defendants disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business as medical groups without adopting reasonable data security measures and complying with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Class members' PII without advising them that Defendants' data security practices were insufficient to maintain the safety and confidentiality of their PII. Accordingly, Plaintiffs and the Class members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

191. Defendants' practices were also contrary to legislatively declared and

public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws like CCRA, CCPA, and FTC Act.

192. The injuries suffered by Plaintiffs and Class members greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiffs and Class members should have reasonably avoided.

193. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs and Class members as a direct result of Defendants' unlawful, unfair, and fraudulent acts and practices as set forth in this Complaint include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their PII;

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

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

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

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

g. damages to and diminution in value of their personal information entrusted to Defendants, and with the understanding that Defendants would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their PII, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect data in their possession.

194. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendants from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VI –- Violation of California Customer Records Act
(By Plaintiffs and the California Subclass)

195. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

196. This count is brought on behalf of all California Subclass members.

197. Cal. Civ. Code § 1798.81.5 of the California Customer Records Act ("CCRA") provides that "to ensure that personal information about California residents is protected," businesses maintaining the personal information of California residents "shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

198. Defendants failed to take reasonable measures to protect Plaintiffs' and

Class members' PII, in violation of Cal. Civ. Code § 1798.81.5.

199. Further, the CCRA requires that "[a] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

200. Defendants did not immediately notify Plaintiffs and the California Subclass of the Data Breach upon their discovery, and instead waited almost two months to provide notice.

201. Defendants also failed to timely and fully disclose the extent of the Data Breach in the Notice sent to Plaintiffs and Class members, in violation of Cal. Civ. Code § 1798.82.

202. Defendants' violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82 are a direct and proximate result of the Data Breach.

203. Plaintiffs and California Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendants from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VII –- Violation of the California Consumer Privacy Act
(By Plaintiffs and the California Subclass)

204. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

205. This count is brought on behalf of all California Subclass members.

206. Cal. Civ. Code § 1798.150(a) of the California Consumer Privacy Act ("CCPA") provides that "[a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision

(d) of Section 1798.81.5 . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's 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 damages, actual damages, injunctive relief, declaratory relief and any other relief the court deems proper.

207. Plaintiffs are "consumers" as defined by Cal. Civ. Code § 1798.140(g) because they are natural persons who reside in California.

208. Defendants are "business[es]" as defined by Cal. Civ. Code § 1798.140(c) because Defendants are corporations organized for the profit or financial benefit of their shareholders or owners and have gross annual revenues in excess of twenty-five million dollars.

209. Defendants failed to take sufficient and reasonable measures to safeguard their data security systems and protect Plaintiffs' and Class members' highly sensitive personal information and medical data from unauthorized access. Defendants' failure to maintain adequate data protections subjected Plaintiffs' and the Class' nonencrypted and nonredacted sensitive personal information to exfiltration and disclosure by malevolent actors.

210. Defendants' violations of Cal. Civ. Code § 1798.150(a) are a direct and proximate result of the Data Breach.

211. Plaintiffs and California Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendants from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VIII –- Violation of California Confidentiality of Medical Information Act

(By Plaintiffs and the California Subclass)

212. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

213. This count is brought on behalf of all California Subclass members.

214. Cal. Civ. Code §56.10(a) of the California Confidentiality of Medical Information Act ("CMIA") provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

215. The CMIA further requires that "[e]very provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." Cal. Civ. Code §56.101(a).

216. Defendants are a "provider of health care" because they are "organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care." Cal. Civ. Code §56.06(a).

217. Plaintiffs are "patient[s]" because they are "natural person[s], whether or not still living, who received health care services from a provider of health care and to whom medical information pertains." Cal. Civ. Code §56.05(l).

218. Defendants failed to safeguard the protected medical information of Plaintiffs and the Class by maintaining inadequate data security networks, allowing

unauthorized parties to access the protected medical information of Plaintiffs and the Class, and failing to preserve the confidentiality of the protected medical information of Plaintiffs and the Class.

219. Defendants allowed third parties to access, exfiltrate, and disclose Plaintiffs' and Class members' protected health and personal information without their consent or knowledge. Defendants negligently represented that such information would be protected from such unauthorized access.

220. Defendants' violations of Cal. Civ. Code §§ 56.10(a) and 56.101(a) are a direct and proximate result of the Data Breach.

221. Plaintiffs and California Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendants from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT IX –- Violation of State Data Breach Statutes
(By Plaintiffs on behalf of the Class)

222. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

223. This count is brought on behalf of all Class members.

224. Defendants are a corporation that owns, maintains, and records PII, and computerized data including PII, about its current and former patients, including Plaintiffs and Class members.

225. Defendants are in possession of PII belonging to Plaintiffs and Class members and are responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

226. Defendants failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by all applicable State laws.

227. Defendants, knowing and/or reasonably believing that Plaintiffs' and Class members' PII was acquired by unauthorized persons during the Data Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiffs and Class members as required by the following data breach statutes.

228. Defendants' failure to provide timely and accurate notice of the Data Breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), *et seq.*;
b. Ark. Code Ann. § 4-110-105(a), *et seq.*;
c. Cal. Civ. Code § 1798.80, *et seq.*;
d. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;
e. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq.*;
f. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq.*;
g. D.C. Code § 28-3852(a), *et seq.*;
h. Fla. Stat. Ann. § 501.171(4), *et seq.*;
i. Ga. Code Ann. § 10-1-912(a), *et seq.*;
j. Haw. Rev. Stat. § 487N-2(a), *et seq.*;
k. Idaho Code Ann. § 28-51-105(1), *et seq.*;
l. Illinois Statute 815 ILCS 530/1, *et seq.*;
m. Iowa Code Ann. § 715C.2(1), *et seq.*;
n. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;
o. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;
p. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;
q. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;
r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), *et seq.*;
s. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;
t. Minn. Stat. Ann. § 325E.61(1)(a), *et seq.*;
u. Mont. Code Ann. § 30-14-1704(1), *et seq.*;
v. Neb. Rev. Stat. Ann. § 87-803(1), *et seq.*;

w. Nev. Rev. Stat. Ann. § 603A.220(1), *et seq.*;

x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;

y. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;

z. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

aa. N.D. Cent. Code Ann. § 51-30-02, *et seq.*;

bb. Okla. Stat. Ann. Tit. 24 § 163(A), *et seq.*;

cc. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;

dd. R.I. Gen. Laws Ann. § 11-49.3-4(a)(1), *et seq.*;

ee. S.C. Code Ann. § 39-1-90(A), *et seq.*;

ff. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

gg. Tex. Bus. & Com. Code Ann. § 521.053(b), *et seq.*;

hh. Utah Code Ann. § 13-44-202(1), *et seq.*;

ii. Va. Code. Ann. § 18.2-186.6(B), *et seq.*;

jj. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*;

kk. Wis. Stat. Ann. § 134.98(2), *et seq.*; and

ll. Wyo. Stat. Ann. § 40-12-502(a), *et seq.*

229. As a result of Defendants' failure to reasonably safeguard Plaintiffs' and Class members' PII, and the failure to provide reasonable and timely notice of the Data Breach to Plaintiffs and Class members, Plaintiffs and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendants' possession, and are entitled to damages in an amount to be proven at trial.

COUNT X – Violation of State Consumer Protection Statutes
(On behalf of Plaintiffs and the Class)

230. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

231. This count is brought on behalf of all Class members.

232. Defendants are a "person" as defined in the relevant state consumer

statutes.

233. Defendants engaged in the conduct alleged herein that was intended to result, and which did result, in the trade and commerce with Plaintiffs and Class members. Defendants are engaged in, and their acts and omissions affect, trade and commerce. Further, Defendants' conduct implicates consumer protection concerns generally.

234. Defendants' acts, practices and omissions were done in the course of Defendants' business of marketing, facilitating, offering for sale, and selling goods and services throughout the United States.

235. Defendants' unlawful, unfair, deceptive, fraudulent and/or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' PII, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including but not limited to duties imposed by the FTC Act and similar state laws, rules, and regulations, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law, statutory,

and self-imposed duties pertaining to the security and privacy of Plaintiffs' and the Class members' PII;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Class members' PII;

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Class members' PII; and

h. Failing to promptly and adequately notify Plaintiffs and Class members that their PII was accessed by unauthorized persons in the Data Breach.

236. By engaging in such conduct and omissions of material facts, Defendants have violated state consumer laws prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," representing that "goods and services are of a particular standard, quality or grade, if they are of another", and/or "engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding"; and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

237. Defendants' representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of Defendants' data security and ability to protect the confidentiality of PII.

238. Defendants intentionally, knowingly, and maliciously misled Plaintiffs and Class members and induced them to rely on their misrepresentations and omissions.

239. Had Defendants disclosed that their data systems were not secure and, thus, vulnerable to attack, they would have been unable to continue in business and

they would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Class members' PII without advising that Defendants' data security practices were insufficient to maintain the safety and confidentiality of their PII. Accordingly, Plaintiffs and the Class members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

240. Past breaches within the industry put Defendants on notice that their security and privacy protections were inadequate.

241. Defendants' practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws like the CCRA, the UCL, and the FTC Act.

242. The harm these practices caused to Plaintiffs and Class members outweighed their utility, if any.

243. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs and Class members as a direct result of Defendants' unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices as set forth herein include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their PII;

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

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

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

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

g. damages to and diminution in value of their personal and medical information entrusted to Defendants and with the understanding that Defendants would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their PII, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect data in its possession.

244. Defendants' conduct described herein, including without limitation, Defendants' failure to maintain adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII, Defendants' failure to disclose the material fact that they did not have adequate computer systems and safeguards to adequately protect Plaintiffs' and Class members' PII, Defendants' failure to provide timely and accurate notice to of the material fact of the Data Breach, and Defendants' continued acceptance of Plaintiffs' and Class members' PII constitutes unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices in violation of the following state

consumer statutes:

a. The Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5(5), (7) and (27), *et seq*.;

b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

c. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107(a)(1)(10) and 4-88-108(1)(2), *et seq*.;

d. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*., and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq.*;

e. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), *et seq*.;

f. The Delaware Deceptive Trade Practices Act, Del. Code Ann. Title 6, § 2532(5) and (7), *et seq*., and the Delaware Consumer Fraud Act, Del. Code Ann. Title 6 § 2513, *et seq*.;

g. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq*.;

h. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-393(a) and (b)(2), (5) and (7), *et seq.*;

i. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), *et seq.*; and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), *et seq.*;

j. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), *et seq.*; and Idaho Code § 48-603C, *et seq.*;

k. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq.*;

l. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-3(a) and (b)(1) and (2), *et seq.*;

m. The Iowa Consumer Fraud Act, I.C.A. §§ 714H.3 and 714H.5, *et seq.*;

n. The Kansas Consumer Protection Act, Kan. Stat. §§ 50-626(a) and (b)(1)(A)(D) and (b)(3), *et seq.*;

o. The Kentucky Consumer Protection Act, K.R.S. § 367.170(1) and (2), *et seq.*;

p. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), *et seq.*;

q. The Maine Uniform Deceptive Trade Practices Act, 10 M.R.S.A. §§ 1212(1)(E) and (G), e*t seq.*, and the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207, *et seq.*;

r. The Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), and (iv) and (9)(i), *et seq.*;

s. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), *et seq.*;

t. The Michigan Consumer Protection Act, M.C.P.L.A. § 445.903(1)(c)(e),(s) and (cc), *et seq.*;

u. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), et seq., the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(a);

v. The Mississippi Consumer Protection Act, Miss. Code Ann. §§ 75-24-5(1), (2)(e) and (g), *et seq.*;

w. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq.*;

x. The Montana Unfair Trade Practices and Consumer Protection Act, MCA §§ 30-14-103, *et seq.*;

y. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), *et seq.*;

z. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915(5) and (7), *et seq.*;

aa. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2(v) and (vii), *et seq.*;

bb. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*;

cc. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7) and (14) and 57-12-3, *et seq.*;

dd. New York Business Law, N.Y. Gen. Bus. Law § 349(a);

ee. The North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), *et seq.*;

ff. The North Dakota Unlawful Sales or Advertising Practices Act, N.D. Cent. Code § 51-15-02, *et seq.*;

gg. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.02(A) and (B)(1) and (2), *et seq.*;

hh. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. § 753(5), (7) and (20), *et seq.*; and the Oklahoma Deceptive Trade Practices Act, 78 Okl. Stat. Ann. § 53(A)(5) and (7), *et seq.*;

ii. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(e)(g) and (u), *et seq.*;

jj. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq.*;

kk. The Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1(6)(v), (vii), (xii), (xiii) and (xiv), *et seq.*;

ll. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), *et seq.*;

mm. The South Dakota Deceptive Trade Practices Act and Consumer Protection Act, S.D. Codified Laws § 37-24-6(1), *et seq.*;

nn. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-

104(a) and (b)(5) and (7);

oo. The Texas Deceptive Trade Practices- Consumer Protection Act, V.T.C.A., Bus. & C. § 17.46(a), (b)(5) and (7), *et seq*.;

pp. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-4(1) and (2)(a) and (b);

qq. The Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a), *et seq.*;

rr. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(5)(6) and (14), *et seq.*;

ss. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq*.;

tt. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, *et seq*.;

uu. The Wisconsin Deceptive Trade Practices Act, W.S.A. § 100.20(1), *et seq.*; and

vv. The Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-105(a), (i), (iii) and (xv), *et seq*.

245. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendants from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT XI –- Intrusion Upon Seclusion

(By Plaintiffs on behalf of the Class, or, in the alternative, the California Subclass)

246. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

247. This count is brought on behalf of all Class members.

248. Plaintiffs bring this claim on behalf of persons who reside in Alabama,

Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia; and any other state that recognizes a claim for intrusion upon seclusion under the facts and circumstances alleged above (the "Intrusion Upon Seclusion States").

249. Plaintiffs and Class members had a reasonable expectation of privacy in the PII that Defendants possessed and/or continues to possess.

250. By failing to keep Plaintiffs' and Class members' PII safe, and by misusing and/or disclosing their PII to unauthorized parties for unauthorized use, Defendants invaded Plaintiffs' and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiffs and Class members, which is highly offensive to a reasonable person.

251. Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' position would consider Defendants' actions highly offensive.

252. Defendants invaded Plaintiffs' and Class members' right to privacy and intruded into Plaintiffs' and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

253. As a proximate result of such misuse and disclosures, Plaintiffs' and Class members' reasonable expectation of privacy in their PII was unduly frustrated and thwarted. Defendants' conduct amounted to a serious invasion of Plaintiffs' and Class members' protected privacy interests.

254. In failing to protect Plaintiffs' and Class members' PII, and in misusing

and/or disclosing their PII, Defendants have acted with malice and oppression and in conscious disregard of Plaintiffs' and the Class members rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its millions of patients. Plaintiffs, therefore, seeks an award of damages, including punitive damages, on behalf of Plaintiffs and the Class.

COUNT XII –- Unjust Enrichment

(By Plaintiffs on behalf of the Class, or, in the alternative, the California Subclass)

255. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

256. This count is brought on behalf of all Class members.

257. Plaintiffs and the Class have an interest, both equitable and legal, in their PII and medical information that was collected and maintained by Defendants.

258. Defendants were benefitted by the conferral upon it of Plaintiffs' and Class members' PII and by their ability to retain and use that information. Defendants understood that it was in fact so benefitted.

259. Defendants also understood and appreciated that Plaintiffs' and Class members' PII and medical information was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that information.

260. But for Defendants' willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class members would not have provide or authorized their PII to be provided to Defendants, and Defendants would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that their data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining patients, gaining the reputational advantages conferred upon it by Plaintiffs and Class

members, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

261. As a result of Defendants' wrongful conduct as alleged herein (including, among other things, their deception of Plaintiffs, the Class, and the public relating to the nature and scope of the data breach; their failure to employ adequate data security measures; their continued maintenance and use of the PII belonging to Plaintiffs and Class members without having adequate data security measures; and its other conduct facilitating the theft of that PII) Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class.

262. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class members' sensitive PII, while at the same time failing to maintain that information secure from intrusion.

263. Under the common law doctrine of unjust enrichment, it is inequitable for Defendants to be permitted to retain the benefits they received, and are still receiving, without justification, from Plaintiffs and the Class in an unfair and unconscionable manner. Defendants' retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

264. The benefit conferred upon, received, and enjoyed by Defendants was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendants to retain the benefit.

265. Defendants are therefore liable to Plaintiffs and the Class for restitution in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically the value to Defendants of the PII and medical information that was accessed and exfiltrated in the Data Breach and the profits Defendants receive from the use and sale of that information.

COUNT XIII –- Declaratory Judgment

(By Plaintiffs on behalf of the Class, or, in the alternative, the California Subclass)

266. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

267. This count is brought on behalf of all Class members.

268. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described herein.

269. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' PII, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their PII. Plaintiffs allege that Defendants' data security measures remain inadequate.

270. Plaintiffs and the Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

271. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendants continue to owe a legal duty to secure Plaintiffs' and Class members' PII, to timely notify them of any data breach, and to establish and implement data security measures that are adequate to secure PII.

272. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect Plaintiffs' and Class members' PII.

273. If an injunction is not issued, Plaintiffs and the Class will suffer

irreparable injury and lack an adequate legal remedy. The threat of another breach of the PII in Defendants' possession, custody, and control is real, immediate, and substantial. If another breach of Defendants' network, systems, servers, or workstations occurs, Plaintiffs and the Class will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

274. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another massive data breach occurs at Defendants, Plaintiffs and the Class will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

275. Issuance of the requested injunction will serve the public interest by preventing another data breach at Defendants, thus eliminating additional injuries to Plaintiffs and the thousands of Class members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendants, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;

B. That Plaintiffs be granted the declaratory relief sought herein;

C. That the Court grant permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices

described herein;

D. That the Court award Plaintiffs and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court award Plaintiffs and the Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

F. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate;

H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the putative Class, demand a trial by jury on all issues so triable.

Date: February 28, 2023

Respectfully Submitted,

By: */s/ Jonathan M. Rotter*

Jonathan M. Rotter (SBN 234137)
Pavithra Rajesh (SBN 323055)
GLANCY PRONGAY & MURRAY LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
jrotter@glancylaw.com
prajesh@glancylaw.com

Daniel O. Herrera (*pro hac vice* anticipated)
Nickolas J. Hagman (*pro hac vice* anticipated)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Bryan L. Clobes (*pro hac vice* anticipated)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
205 N. Monroe St.
Media, PA 19063
Telephone: (215) 864-2800
Facsimile: (312) 782-4485
bclobes@caffertyclobes.com

Attorneys for Plaintiffs and the Proposed Class

ClassAction.org