ZIMMERMAN REED LLP
Caleb Marker (SBN 269721)
E-mail: caleb.marker@zimmreed.com
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
(877) 500-8780 Telephone
(877) 500-8781 Facsimile

ZIMMERMAN REED LLP
Brian C. Gudmundson (*pro hac vice* forthcoming)
E-mail: brian.gudmundson@zimmreed.com
Jason P. Johnston (*pro hac vice* forthcoming)
E-mail: jason.johnston@zimmreed.com
Michael J. Laird (*pro hac vice* forthcoming)
E-mail: michael.laird@zimmreed.com
Rachel K. Tack (*pro hac vice* forthcoming)
E-mail: rachel.tack@zimmreed.com
80 S 8th Street, Suite 1100
Minneapolis, MN 55402
(612) 341-0400 Telephone
(612) 341-0844 Facsimile

THE JOHNSON FIRM
Christopher D. Jennings (*pro hac vice* forthcoming)
E-mail: chris@yourattorney.com
610 President Clinton Avenue
Suite 300
Little Rock, AR 72201
(501) 372-1300 Telephone

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

SAM ABEDI and FARNAZ DOROODIAN, on behalf of themselves and all others similarly situated, Plaintiffs, v. HERITAGE PROVIDER NETWORK, INC. and REGAL MEDICAL GROUP, INC. Defendants	CASE NO.: 2:23-cv-1113 **COMPLAINT** 1. Negligence 2. Negligence *per se* 3. Violation of California Consumer Privacy Act of 2018 4. Violation of the Unfair Competition Law (Plaintiff Demands Trial by Jury)

INTRODUCTION

Plaintiffs Sam Abedi and Farnaz Doroodian ("Plaintiffs"), by and through their attorneys of record, upon personal knowledge as to their own acts and experiences, and upon information and belief as to all other matters, files this complaint against Heritage Provider Network, Inc. and Regal Medical Group, Inc. (collectively, "HPN" or "Defendants") and alleges the following:

INTRODUCTION

1. Plaintiffs bring this class action complaint on behalf of a class of individuals impacted by Defendants' failure to safeguard, monitor, maintain and protect highly sensitive Personal Health Information ("PHI") and Personally Identifiable Information ("PII") (collectively "Sensitive Information"). Defendants collected, stored, maintained Plaintiffs' and the Class's Sensitive Information as part of its ordinary business activities as a medical group provider.

2. In or around December 1, 2022, four medical groups owned or operated by or otherwise affiliated with Defendants—Regal Medical Group, Lakeside Medical organization, ADOC Medical Group, and Greater Covina Medical—were impacted by a cyberattack during which criminal hackers obtained access to and ultimately stole Plaintiffs' and the Class's Sensitive Information ("Data Breach").[1] Defendants discovered the Data Breach on December 8, 2022, several days after having experienced difficulties accessing their servers, including servers maintaining patients' Sensitive Information. During the Data Breach, criminal hackers entered into and obtained control over Defendants' servers, providing them access to Plaintiffs' and the Class's Sensitive Data. Defendants' investigation of the Data Breach revealed that the intrusion began in or around December 1, 2022, and that the criminal hackers successfully exfiltrated patient information out of Defendants' control.

[1] An exemplar Notice of the Data Breach Defendants sent to Plaintiff Farnaz Doroodian is attached as Exhibit A.

3. Although the Data Breach began in December of 2022 and despite Defendants' knowledge that the hackers stole patient information, Defendants waited until February 1, 2023, to notify the impacted patients, a delay of approximately two months. The Data Breach notice admitted that Defendants experienced a cyberattack that exposed highly Sensitive Information, including patient: names, Social Security numbers, dates of birth, addresses, diagnostic and treatment information, laboratory test results, prescription data, radiology reports, health plan member numbers, and phone numbers.

4. Hackers highly target this type of highly sensitive information because that type of information can be used to orchestrate a host of fraudulent activities, including medical and insurance fraud, financial fraud, and identity theft. Often, the entire purpose of these types of medical data breaches is to misuse the stolen information or to sell it to fraudsters on the dark web.

5. Defendants have estimated over 3 million patients were impacted by the Data Breach. Consequently, millions of individuals are at a heightened, continued, and significant risk that their information will misused for attempted or actual fraud or identity theft.

6. Plaintiffs and the Class face that significant and lasting risk of harm because of Defendants' inadequate data security. Indeed, this type of Data Breach is only possible where Defendants' had implemented and used inadequate data security measures. Indeed, the hackers' ability to access the system, escalate their privileges within the systems, gain access to servers containing patients' Sensitive Information, and exfiltrate that information out of the servers indicates multiple levels of security failures at every stage of the Data Breach.

7. As a result of Defendants' conduct, Plaintiffs and the Class have and will be required to continue to undertake time-consuming and, often costly, efforts to mitigate the actual and potential harm caused by the Data Breach's exposure of their Sensitive Information, including by, among other things: (1)placing freezes and alerts with credit reporting agencies , contacting their financial institutions, closing or modifying financial

accounts, reviewing and monitoring their credit reports and accounts for unauthorized activity, changing passwords on potentially impacted websites and applications, and requesting and maintaining accurate medical records. Minors may not be able to monitor the impact of the Data Breach on their lives for years, at which point the damage will be done.

8. As such, Plaintiffs and the Class bring this action to recover for the harm they suffered, and assert the following claims: negligence, negligence *per se*, violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, and violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*.

JURISDICTION AND VENUE FOR FEDERAL COURT

9. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, the plaintiffs class includes all recipients of Defendants' notice of the Data Breach, which, upon information and belief, includes non-California citizens. Since Defendants are both California entities that are headquartered in California, there is minimal diversity between at least one member of the plaintiff class and Defendants.

10. This Court has general personal jurisdiction over Defendant because Defendant operates its principal place of business in this State. Additionally, this Court also has specific personal jurisdiction over Defendant because it has minimum contacts with this State, as it is located and conducts substantial business here, and Plaintiffs' claims arise from Defendant's conduct in this State.

11. This Court is the proper venue for this action pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to

Plaintiffs' claims occurred in this District and because Defendant conducts a substantial part of its business within this District.

PARTIES

12. **Plaintiff** Sam Abedi is a citizen of California residing in Woodland Hills, California. He is a member of Defendants' medical group and has received medical services from providers within Defendants' medical network. To receive those services, Plaintiff provided his medical providers with personal and medical information, which the providers in turn gave to Defendants. On February 6, 2023, he was sent a Notice of Data Breach letter by Defendants stating that his information may have been impacted by the Data Breach.

13. **Plaintiff** Farnaz Doroodian is a citizen of California residing in Woodland Hills, California. She is a member of Defendants' medical group and has received medical services from providers within Defendants' medical network. To receive those services, Plaintiff provided her medical providers with personal and medical information, which the providers in turn gave to Defendants. On February 1, 2023, she was sent a Notice of Data Breach letter by Defendants stating that her information may have been impacted by the Data Breach.

14. **Defendant** Heritage Provider Network, Inc. ("HPN") is a California Company headquartered in Northridge, California. HPN administers health care groups in California, including, but not limited to, Regal Medical Group, ADOC Medical Group, and Lakeside Medical Group.

15. **Defendant** Regal Medical Group ("Regal") is a California a California entity headquartered in Reseda, California. HPN administers Regal, and Regal is affiliated with ADOC Medical Group, Lakeside Medical Group, and Greater Covina Medical Group, Inc. Regal issued the Notice of Data Breach in conjunction with ADOC Medical Group, Lakeside, Medical Group, and Greater Covina Medical Group.

FACTUAL BACKGROUND

A. Defendants Collected, Maintained and Stored Sensitive Information

16. HPN administers a serious of medical groups, including, but not limited to, Regal, ADOC Medical Group, and Lakeside Medical Group. Upon information and belief, Covina Medical Group, Inc., is affiliated with Regal.

17. Collectively, HPN and Regal operate as medical groups that connect individuals with their health plans, and provide a network of primary care physicians, specialists, hospitals, urgent care centers, and labs for members to use.

18. As part of Defendants services, Defendants obtain highly sensitive personal and medical information from plan members.

19. To obtain healthcare services, patients, like Plaintiffs and the Class, must provide their medical providers with highly sensitive information, including PHI, PII, or both. Those providers, in turn, share that data with Defendants, who then compiles, stores, and maintains the highly sensitive PII and PHI. As a massive medical group, Defendants serve millions of patients by acting as the intermediary between patients, their health plans, and their medical providers. Defendants, as a result, have collected and maintained a massive repository of Sensitive Information, acting as a particularly lucrative target for data thieves looking to obtain and misuse or sell patient data.

20. Plaintiffs and the Class had a reasonable expectation that Defendants would protect the Sensitive Information that it collected and maintained, especially because, given the publicity of other data breaches and the significant impact they have had on patients and other consumers, Defendants knew or should have known that failing to adequately protect patient information could cause substantial harm.

21. Additionally, Defendants each have a Notice of Privacy Practices that are nearly identical. Both acknowledge that each is "required by law to maintain the privacy and security of your protected health information" and to "let you know promptly if a

breach occurs that may have compromised the privacy or security of your information."[2] Regal also acknowledges its responsibilities under HIPAA, including its obligations to safeguard data.

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

B. Defendants Suffered a Massive Data Breach Exposing Patients' Sensitive Information

23. On or around December 1, 2022, a malicious actor gained unauthorized access to Defendants' servers. Through a series of escalations, the hackers later gained access to the sensitive personal, medical, financial, and insurance information of Defendants' current and former patients. The malicious actors maintained unfettered access to Defendants' servers until Defendants remediated the breach and resolved its security vulnerabilities during the Data Breach, the hackers copied and exfiltrated substantial amounts of Plaintiffs' and the Class's PII and PHI.

24. Defendants did not disclose the existence of the Data Breach to its patients or the public until February 1, 2023, nearly two months after it initially learned of the Data Breach. The Notice warned patients that the following information had been stolen by malicious actors during the Data Breach: names, social security numbers, addresses, dates of birth, diagnoses and treatments, laboratory test results, prescription data, radiology reports, health plan member numbers, and phone numbers. Defendants also posted a notice of the Data Breach on its website.

[2] https://www.regalmed.com/Regal-en-us/assets/File/RMG-Notice-of-Privacy-Practice.pdf; https://www.heritageprovidernetwork.com/files/Privacy%20Practice.pdf

25. The Data Breach notices recommended Plaintiffs and the Class take several time-consuming steps to "help protect [your] identity," including "register a fraud alert," "monitor account statements" and "contact your state Consumer Protection Agency[.]"

26. Given that Defendants were storing the PII and PHI of Plaintiffs and the Class and knew or should have known of the serious risk and harm caused by a data breach, Defendants were obligated to implement reasonable measures to prevent and detect cyber-attacks, such as those recommended by the Federal Trade Commission, required by the Health Insurance Portability and Accountability Act, and promoted by data security experts and other agencies. That obligation stems from the foreseeable risk of a Data Breach given that Defendants collected, stored, and had access to a swath of highly sensitive patient records and data and, additionally, because other highly publicized data breaches at different healthcare institutions put Defendants on notice that the higher personal data they stored might be targeted by cybercriminals.

27. Despite the highly sensitive nature of the information Defendants obtained, maintained, and stored, and the prevalence of health care data breaches, Defendants inexplicably failed to take appropriate steps to safeguard the PII and PHI of Plaintiffs and the Class from being compromised. The Data Breach itself, and information Defendants have disclosed about the breach to date, including its length, the need to remediate Defendants' cybersecurity, the number of people impacted, and the sensitive nature of the impacted data collectively demonstrate Defendants failed to implement reasonable measures to prevent cyber-attacks and the exposure of the Sensitive Information it oversaw.

C. Exposure of Sensitive Information Creates a Substantial Risk of Harm

28. The personal, health, and financial information of Plaintiffs and the Class is valuable and has become a highly desirable commodity to data thieves.

29. Defendants' failure to reasonably safeguard Plaintiffs' and the Class's sensitive PHI and PII has created a serious risk to Plaintiffs and the Class, including both a short-term and long-term risk of identity theft.

30. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

31. According to experts, one out of four data breach notification recipients becomes a victim of identity fraud.[3]

32. Stolen Sensitive Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines and is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal identities and online activity.

33. Additionally, Defendants' Data Breach impacted minors' sensitive personal and medical information. According to Robert P. Chappell, Jr., a law enforcement professional, fraudsters can steal and use a minor's information until the minor turns eighteen years old before the minor even realizes he or she has been the victim of an identity theft crime.[4]

34. The risk to minor Class members is substantial given their age and lack of established credit. The information can be used to create a "clean slate identity," and use that identity for obtaining government benefits, fraudulent tax refunds, and other scams. There is evidence that children are 51% more likely to be victims of identity theft than adults.[5]

---

[3] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims,* ThreatPost.com (last visited Jan. 17, 2022), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/

[4] Brett Singer, *What is Child Identity Theft?*, Parents (last visited Jan. 17, 2022), https://www.parents.com/kids/safety/tips/what-is-child-dentity-theft/.

[5] Avery Wolfe, *How Data Breaches Affect Children*, Axion Cyber Sols. (Mar. 15, 2018) (last visited Jan. 18, 2022), https://axioncyber.com/data-breach/how-data-breaches-affect-children/.

35. Purchasers of Sensitive Information use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. This can result in the discovery and release of additional Sensitive Information from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass financial data and tangible money, along with unreported emotional harms.

36. The FBI's Internet Crime Complaint (IC3) 2019 estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. The same report identified "rapid reporting" as a tool to help law enforcement stop fraudulent transactions and mitigate losses.

37. Defendants did not rapidly, or even reasonably, report to Plaintiffs and the Class that their Sensitive Information had been exposed or stolen.

38. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[6]

39. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require:

(1) encrypting information stored on computer networks;

(2) retaining payment card information only as long as necessary;

[6] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Jan. 18, 2022) http://www/ftc/gov/speeches/harbour/091207privacyroundtable.pdf.

(3) properly disposing of personal information that is no longer needed or can be disposed pursuant to relevant state and federal laws;

(4) limiting administrative access to business systems;

(5) using industry unapproved activity;

(6) monitoring activity on networks to uncover unapproved activity;

(7) verifying that privacy and security features function property;

(8) testing for common vulnerabilities; and

(9) updating and patching third-party software.[7]

40. The United States Government and the United States Cybersecurity & Infrastructure Security Agency recommend several similar and supplemental measures to prevent and detect cyber-attacks, including, but not limited to: implementing an awareness and training program, enabling strong spam filters, scanning incoming and outgoing emails, configuring firewalls, automating anti-virus and anti-malware programs, managing privileged accounts, configuring access controls, disabling remote desktop protocol, and updating and patching computers.

41. The FTC cautions businesses that failure to protect Sensitive Information and the resulting data breaches can destroy consumers' finances, credit history, and reputations, and can take time, money and patience to resolve the effect.[8] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures—like Defendants failed to do here—as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

[7] *Start With Security, A Guide for Business,* FTC (last visited Jan. 18, 2022) https://www.ftc.gov/system/files/documents/plain-language/pdf0205.

[8] *See* Taking Charge, What to Do if Your Identity is Stolen, FTC, at 3 (2012) (last visited Jan. 19, 2022), www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

D. The Healthcare Industry is Particularly Susceptible to Cyber Attacks.

42. A 2010 report focusing on healthcare data breaches found the "average total cost to resolve an identity theft related incident … came to about $20,000."[9] According to survey results and population extrapolations from the National Study on Medical Identity Theft report from the Ponemon Institute, nearly 50% of victims reported losing their healthcare coverage because of a data breach and nearly 30% reported an increase in their insurance premiums.[10] Several individuals were unable to fully resolve their identity theft crises. Healthcare data breaches are an epidemic and they are crippling the impacted individuals—millions of victims every year.[11]

43. According to an analysis of data breach incidents reported to the U.S. Department of Health and Human Services and the media, from 2015 and 2019, the number of healthcare related security incidents increased from 450 annual incidents to 572 annual incidents, likely a conservative estimate.[12]

44. According to the Verizon Data Breach Investigations Report, the health care industry, including hospitals and other providers, experienced 655 known data breaches,

[9] *See* Elinor Mills, *Study: Medical identity theft is costly for victims,* CNET (March 3, 2010), (last visited Jan. 11, 2021), https://www.cnet.com/tech/services-and-software/study-medical-identity-theft-is-costly-for-victims/

[10] *Id.*

[11] *Id.*

[12] Heather Landi, *Number of patient records breached nearly triples in 2019*, FIERCE HEALTHCARE (Feb. 20, 2020), https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats#:~:text=OVer%2041%20million%20patient%20records,close%20to%2021%20million%20records (last visited Jan.19, 2022).

472 of which had confirmed data disclosures in 2021.[13] For the tenth year in a row, the healthcare industry has seen the highest impact from cyber-attacks of any industry.[14]

45. As a healthcare provider with numerous medical facilities and hundreds of thousands of patients, if not more, Defendants knew or should have known the importance of protecting the Sensitive Information entrusted to it. Defendants also knew or should have known of the foreseeable, and catastrophic consequences if its systems were breached. These consequences include substantial costs to Plaintiffs and the Class because of the Data Breach. Despite this, Defendants failed to take reasonable data security measures to prevent or mitigate losses from cyberattacks.

E. Plaintiffs' and the Class's PHI and PII are Valuable.

46. Unlike financial information, such as credit card and bank account numbers, the PHI and certain PII exfiltrated in the Data Breach cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or her life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable to hackers.[15]

47. Birth dates, Social Security numbers, addresses, employment information, income, and similar types of information can be used to open several credit accounts on

---

[13] Verizon, 2021 Data Breach Investigations Report: Healthcare NAICS 62 (2021) (last visited Jan. 19, 2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/healthcare-data-breaches-security/.

[14] *Five worthy reads: The never-ending love story between cyberattacks and healthcare,* ManageEngine, https://blogs.manageengine.com/corporate/manageengine/2021/08/06/the-never-ending-love-story-between-cyberattacks-and-healthcare.html#:~:text=According%20to%20Infosec%20Institute%2C%20credit,is%20%24158%20per%20stolen%20record.

[15] *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited Jan. 18, 2022).

an ongoing basis rather than exploiting just one account until it's canceled.[16] For that reason, Cybercriminals on the dark web are able to sell Social Security numbers for large profits. For example, an infant's social security number sells for as much as $300 per number.[17] Those numbers are often then used for fraudulent tax returns.[18]

48. Consumers place a considerable value on their Sensitive Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between $30.49 and $44.62.[19] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

49. Defendants' Data Breach exposed a variety of Sensitive Information, including Social Security numbers and PHI.

50. The Social Security Administration ("SSA") warns that a stolen Social Security number can lead to identity theft and fraud: "Identity thieves can use your number and your credit to apply for more credit in your name."[20] If the identity thief applies for credit and does not pay the bill, it will damage victims' credit and cause a series of other related problems.

---

[16] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[17] *Id.*

[18] *Id.*

[19] 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore,* at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Jan. 19, 2022).

[20] Social Security Administration, *Identity Theft and Your Social Security Number*, (last visited Jan. 19, 2022), https://www.ssa.gov/pubs/EN-05-10064.pdf.

51. Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

52. PHI, also at issue here, is likely even more valuable than Social Security numbers and just as capable of being misused. The Federal Bureau of Investigation ("FBI") has found instances of PHI selling for fifty times the price of stolen Social Security numbers or credit card numbers.[21]

53. Other reports found that PHI is ten times more valuable on the black market than credit card information.[22] This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, social security numbers. Credit card information and PII sell for $1-2 on the black market, but PHI can sell for as much as $363 according to the Infosec Institute.[23]

54. Cybercriminals recognize and exploit the value of PHI and PII. The value of PHI and PII is the foundation to the cyberhacker business model.

55. Because the Sensitive Information exposed in the Defendants' Data Breach is permanent data, there may be a gap of time between when it was stolen and when it will be used. The damage may continue for years. Plaintiffs and the Class now face years of monitoring their financial and personal records with a high degree of scrutiny.

---

[21] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-healthcare-cyber-intrusions/ (last visited Jan. 18, 2022).

[22] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[23] *Hackers Selling Healthcare Data in the Black Market*, INFOSEC, https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 18, 2022).

The Class has incurred and will incur this damage in additional to any fraudulent use of their Sensitive Information.

F. Defendants' Conduct Violates HIPAA

56. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), individuals' health information must be:

> properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.[24]

57. HIPAA is a "federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[25] The rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.[26]

58. HIPAA defines sensitive patient personal and health information as: (1) Name; (2) Home and work addresses; (3) Home and work phone numbers; (4) Personal and professional email addresses; (5) Medical records; (6) Prescriptions; (7) Health insurance information; (8) Billing information; (9) Social Security number; (10) Spouse and children's information; and/or (11) Emergency contact information.[27]

59. To ensure protection of this private and sensitive information, HIPAA mandates standards for handling PHI—the very data Defendants failed to protect. The Data Breach resulted from Defendants' failure to comply with several of these standards:

---

[24] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Jan. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[25] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Jan. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/security/index.html.

[26] *Id.*

[27] *Id.*

a. Violation of 45 C.F.R. § 164.306(a)(1): failing to ensure the confidentiality and integrity of electronic protected health information that Defendants created, received, maintained, and transmitted;

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

c. Violation of 45 C.F.R. § 164.308(a)(1): Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

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

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

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

g. Violation of 45 C.F.R. §164.306(a)(94): Failing to ensure compliance with HIPAA security standard rules by its workforce;

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

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

60. Despite Defendants' failure to reasonably protect Plaintiffs' and the Class's Sensitive Information, it has not offered any compensation or adequate remedy considering the significant and long-term risk Plaintiffs and the Class face.

CLASS ALLEGATIONS

61. Plaintiffs brings this class action pursuant to Federal Rule Civil Procedure 23 on behalf of themselves and all others similar situated, as representative of the following Class:

> All persons who received or were otherwise sent notice that they were impacted by Defendants' Data Breach.

62. Excluded from the Class are Defendants; its officers, directors, and employees of Defendant; any entity in which Defendants have a controlling interest in, is a parent or subsidiary of, or which is otherwise controlled by Defendant; and Defendants' affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assignees. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

63. Plaintiffs reserve the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

64. All members of the proposed Class are readily identifiable through Defendants' records.

65. **Numerosity.** The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiffs are informed and believes that the proposed Class includes at least 3 million people. The precise number of Class members is unknown to Plaintiffs but may be ascertained from Defendants' records.

66. **Commonality and Predominance.** This action involves common questions of law and fact to the Plaintiffs and Class members, which predominate over any questions only affecting individual Class members. These common legal and factual questions include, without limitation:

a. Whether Defendants owed Plaintiffs and the other Class members a duty to adequately protect their Sensitive Information;

b. Whether Defendants owed Plaintiffs and the other Class members a duty to implement reasonable data security measures due to the foreseeability of a data breach;

c. Whether Defendants owed Plaintiffs and the other Class members a duty to implement reasonable data security measures because Defendants accepted, stored, and maintained highly sensitive information concerning Plaintiffs and the Class;

d. Whether Defendants knew or should have known of the risk of a data breach;

e. Whether Defendants breached its duty to protect the PII and PHI of Plaintiffs and other Class members;

f. Whether Defendants knew or should have known about the inadequacies of its data protection, storage, and security;

g. Whether Defendants failed to use reasonable care and reasonable methods to safeguard and protect Plaintiffs' and the Class's Sensitive Information from unauthorized theft, release, and disclosure;

h. Whether proper data security measures, policies, procedures and protocols were in enacted within Defendants' offices and computer systems to safeguard and protect Plaintiffs' and the Class's Sensitive Information from unauthorized theft, release or disclosure;

i. Whether Defendants' conduct was the proximate cause of Plaintiffs' and the Class's injuries;

j. Whether Plaintiffs and the Class suffered ascertainable and cognizable injuries as a result of Defendants' misconduct;

k. Whether Plaintiffs and the Class are entitled to recover damages; and

l. Whether Plaintiffs and the Class are entitled to other appropriate remedies including injunctive relief.

67. Defendants engaged in a common course of conduct giving rise to the claims asserted by Plaintiffs on behalf of themselves and the Class. Individual questions, if any, are slight by comparison in both quality and quantity to the common questions that control this action.

68. **Typicality.** Plaintiffs' claims are typical of those of other Class members because Plaintiffs' PHI and PII, like that of every other Class member, was misused and improperly disclosed by Defendants. Defendants' misconduct impacted all Class members in a similar manner.

69. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interest of the members of the Class and have retained counsel experienced in complex consumer class action litigation and intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class.

70. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendants. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court.

CLAIMS

COUNT I
Negligence
(on behalf of Plaintiffs and the Class)

71. Plaintiffs reallege and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

72. Defendants collected, maintained, and stored Plaintiffs' and the Class's Sensitive Information for the purpose of providing medical treatment to Plaintiffs and the Class.

73. Plaintiffs and the Class are a well-defined, foreseeable, and probable group of patients that Defendants were aware, or should have been aware, could be injured by inadequate data security measures. The nature of Defendants' business requires patients to disclose Sensitive Information to receive adequate care, including, but not limited to, medical histories, dates of birth, addresses, phone numbers, and medical insurance information. That information is then exchanged with Defendants by Plaintiffs' and the Class's medical providers for insurance purposes. Therefore, Defendants' use, handle, gather, and store the Sensitive Information of Plaintiffs and the Class and, additionally, solicit and store records containing Plaintiffs' and the Class's Sensitive Information.

74. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Defendants knew or should have known that, given its repository of a host of Sensitive Information For hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Defendants had a duty to reasonably safeguard its patients' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiffs and the Class of inadequate data security created a duty to act reasonably and safeguard the Sensitive Information.

75. Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in safeguarding and protecting their Sensitive Information in its possession from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

76. This duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiffs' and the Class's PHI and PII was adequately protected and secured. Defendants further had a duty to implement processes that would detect a breach of their security system in a timely manner.

77. Defendants also had a duty to timely disclose to Plaintiffs and the Class that their Sensitive Information had been or was reasonably believed to have been compromised. Timely disclosure is necessary so that, among other things, Plaintiffs and the Class may take appropriate measures to begin monitoring their accounts for unauthorized access, to contact the credit bureaus to request freezes or place alerts and take all other appropriate precautions, including those recommended by Defendants.

78. Additionally, HIPAA creates industry standards for maintaining the privacy of health-related data. Defendants knew or should have known it had a legal obligation to secure and protect Plaintiffs and the Class's Sensitive Information and that failing to do so is a serious violation of HIPAA.

79. Defendants also should have known that, given the Sensitive Information it held, Plaintiffs and the Class would be harmed should it suffer a Data Breach. Defendants knew or should have known that their systems and technologies for processing and securing Plaintiffs' and the Class's PHI and PII had security vulnerabilities susceptible to cyber-attacks.

80. Despite that knowledge, Defendants implemented unreasonable data security measures that allowed cybercriminals to successfully breach Defendants' network and data environments, reside there undetected for a significant period of time, and access or steal a host of personal and healthcare information on thousands of Defendants' patients.

81. Defendants, through its actions and/or omissions, failed to provide reasonable security for the data in its possession.

82. Defendants breached is duty to Plaintiffs and the Class by failing to adopt, implement, and maintain reasonable security measures to safeguard their Sensitive Information, allowing unauthorized access to Plaintiffs' and the Class's PHI and PII, and failing to recognize the Data Breach in a timely manner. Defendants further failed to comply with industry regulations and exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class's PHI and PII.

83. But for Defendants' wrongful and negligent breach of its duties, their Sensitive Information would not have been accessed and exfiltrated by unauthorized persons, and they would not face a risk of harm of identity theft, fraud, or other similar harms.

84. As a result of Defendants' negligence, Plaintiffs and the Class suffered damages including, but not limited to, ongoing and imminent threat of identity theft crimes; out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or fraud; credit, debit, and financial monitoring to prevent and/or mitigate theft, identity theft, and/or fraud incurred or likely to occur as a result of Defendants' security failures; the value of their time and resources spent mitigating the identity theft and/or fraud; decreased credit scores and ratings; and irrecoverable financial losses due to fraud.

COUNT II
Negligence *Per Se*
(on behalf of Plaintiffs and the Class)

85. Plaintiffs reallege and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

86. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair ... practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

87. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's PHI and PII and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

88. To provider its services to Plaintiffs' and the Class, Defendants collected, maintained, and stored Plaintiffs' and the Class's Sensitive Information.

89. Additionally, as a healthcare provider, Defendants are covered by HIPAA, 45 C.F.R. § 160.102, and is therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

90. HIPAA, 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information."

91. Per 45 C.F.R. § 164.306, HIPAA "standards, requirements and implementation specifications" apply to covered entities, such as Defendants. HIPAA standards are mandatory.

92. HIPAA requires Defendants to "ensure the confidentiality, integrity, and availability of all electronic protected health information" it receives and to protect against any "reasonably anticipated threats or hazards to the security or integrity" of the Sensitive Information. 45 C.F.R. § 164.306.

93. Defendants violated HIPAA by failing to adhere to and meet the requirements of 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

94. Defendants violated HIPAA by failing to use reasonable measures to protect the PII and PHI of Plaintiffs and Class. Defendants' conduct was especially unreasonable given the nature of the Sensitive Information and the number of patients it serves, some of which are minors or patients who live below the federal poverty level, who may not have the means to expend significant amounts of time and money to fully mitigate the fallout of the Data Breach.

95. Defendants' violation of Section 5 of the FTC Act and HIPAA both separately and individually constitute negligence *per se*.

96. Plaintiffs and the Class are within the group of individuals the FTC Act and HIPAA were designed to protect and the harm to these individuals is a result of the Data Breach. Moreover, the harm that has occurred is the type of harm the FTC Act (and

similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the proposed Class.

97. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class members suffered and continue to suffer injuries and are entitled to damages in an amount to be proven at trial.

98. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have been injured as described herein and are entitled to damages in an amount to be proven at trial.

COUNT III
Violation of the California Consumer Privacy Act of 2018
Civ. Code § 1798.100, *et seq*. (CCPA)
(On behalf of Plaintiffs and the California Class)

99. Plaintiffs reallege and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

100. Section 1798.150(a)(1) of the CCP provides, "[a]ny consumer whose nonencrypted or nonredacted personal information, as defined by [Civil Code section 1798.81.5(d)(1)(A)] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

101. Plaintiffs and proposed Class members are consumers and California residents as defined by Civil Code section 1798.140(g).

102. Defendants are a "business" as defined by Civil Code section 1798.140(c) because it is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with

others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California."

103. Defendants collects personal information from, among other sources, consumers who request and use its educational services.

104. Defendants' servers were compromised in the breach.

105. Plaintiffs' and Class members' personal information, as defined by Civil Code section 1798.81.5(d)(1)(A), was subject to unauthorized access and exfiltration, theft or disclosure. The Data Breach described herein exposed, without limitation, names, Social Security numbers, dates of birth, addresses, diagnostic and treatment information, laboratory test results, prescription data, radiology reports, health plan member numbers, and phone numbers.

106. Defendants maintained Plaintiffs' and Class members' Sensitive Information in a form that allowed criminals to access and exfiltrate it during the Data Breach.

107. The Data Breach occurred as a result of Defendants' failure to implement and maintain reasonable security procedures and practices for protecting the exposed information given its nature. Defendants failed to monitor its systems to identify suspicious activity and allowed unauthorized access to Plaintiffs' and Class members' Sensitive Information. As a result, Plaintiffs suffered harm, including the loss in value, integrity and confidentiality of their PII and the increased risk of future harm, namely, fraud and identity theft resulting from the Data Breach.

108. Accordingly, on behalf of the Class, Plaintiffs injunctive and declaratory relief, and any other relief deemed appropriate by the Court. Concurrent with the filing of this Complaint, Plaintiffs notified Defendants of their alleged violations pursuant to Cal. Civil Code § 1798.150 and issued a demand for relief. If, in 30 days, Defendants do not agree to the relief requested, Plaintiffs will amend the Complaint with 30 days to allege actual and statutory damages.

COUNT IV
Violation of the Unfair Competition Law,
Bus. & Prof. Code § 17200 *et seq.* (UCL)
(Against All Defendants)

109. Plaintiffs reallege and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

110. The UCL proscribes "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

111. Defendants conduct is unlawful, in violation of the UCL, because it violates the CMIA.

112. Defendants' conduct is fraudulent because it omitted, suppressed, and concealed material facts regarding its failure to take reasonable or adequate precautions to secure Plaintiffs' and Class members' personal information. Despite being aware that its systems had vulnerabilities and suffered a cyberattack—which Plaintiffs and Class members had no reasonable means of knowing—Defendants never disclosed that information to Plaintiffs and the Class.

113. Defendants' conduct also is unfair and deceptive in violation of the UCL. Defendants' unfair and fraudulent business acts and practices include:

a. failing to adequately secure the personal information of Plaintiffs and Class members from disclosure to unauthorized third parties or for improper purposes;

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

c. enabling the disclosure of personal and sensitive facts about Plaintiffs and Class members without their informed, voluntary, affirmative, and clear consent; and

d. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and Class members from taking timely self-protection measures.

114. The harm resulting from Defendants' unfair conduct outweighs any potential utility. The failure to adequately safeguard personal, sensitive information harms the public at large and is part of a common and uniform course of wrongful conduct.

115. The harm from Defendants' conduct was not reasonably avoidable by consumers. The individuals affected by the Data Breach – faculty, staff and students – were required to provide their PII as part of their relationship with the relevant Defendants institutions. Plaintiffs and Class members did not know of, and had no reasonable means of discovering, that their information would be exposed to hackers through inadequate data security measures.

116. There were reasonably available alternatives that would have furthered Defendants' business interests of electronically transferring their customers' information while protecting PII, such as using cybersecurity software, active monitoring, employee training and ensuring best practices in cybersecurity defense.

117. Defendants' omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of Plaintiffs' and Class members' personal information. A reasonable person would regard Defendants' negligent data security and the Data Breach as important, material facts. Defendants could and should have timely disclosed these facts.

118. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices, Plaintiffs and Class members were injured, because their sensitive personal information experienced a diminution of value and because they devoted additional time – which they otherwise would or could have devoted to pecuniary gain – to monitoring their credit reports and financial accounts for fraudulent activity.

119. Plaintiffs and Class members therefore seek all monetary and non-monetary relief permitted by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs under Code of Civil Procedure section 1021.5.

PRAYER FOR RELIEF

120. WHEREFORE, Plaintiffs respectfully pray for judgment in their favor as follows:

a. Certification the Class pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and an order that notice be provided to all Class Members;

b. Designation of Plaintiffs as representatives of the Class and the undersigned counsel, Zimmerman Reed LLP, as Class Counsel;

c. An award of damages in an amount to be determined at trial or by this Court;

d. An order for injunctive relief, enjoining Defendants from engaging in the wrongful and unlawful acts described herein;

e. An award of statutory interest and penalties;

f. An award of costs and attorneys' fees; and

g. Such other relief the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

121. Plaintiffs hereby demand a trial by jury of all issues so triable.

Respectfully submitted,

Date: February 14, 2023 By: /s/ Caleb Marker

Caleb Marker (SBN 269721)
ZIMMERMAN REED LLP
6420 Wilshire Blvd., Suite 1080
Los Angeles, CA 90048
Telephone: (877) 500-8780
Facsimile: (877) 500-8781
caleb.marker@zimmreed.com

Brian C. Gudmundson*
Jason P. Johnston*
Michael J. Laird*
Rachel K. Tack*
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
jason.johnston@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com

Christopher D. Jennings*
THE JOHNSON FIRM
610 President Clinton Avenue
Suite 300
Little Rock, AR 72201
Telephone: (501) 372-1300
chris@yourattorney.com

*To be admitted *pro hac vice*

Attorneys for Plaintiffs and the Proposed Class