

1 Rosemary M. Rivas (SBN 209147)  
 2 Steven Lopez (SBN 300540)  
 3 David M. Berger (SBN 277526)  
 4 Rosanne L. Mah (SBN 242628)  
**GIBBS LAW GROUP LLP**  
 5 1111 Broadway, Suite 2100  
 6 Oakland, California 94607  
 7 (510) 350-9700 (tel.)  
 8 (510) 350-9701 (fax)  
 9 rmr@classlawgroup.com  
 10 sal@classlawgroup.com  
 11 dmb@classlawgroup.com  
 12 rlm@classlawgroup.com

*Attorneys for Plaintiff*

11 **UNITED STATES DISTRICT COURT FOR THE**  
 12 **EASTERN DISTRICT OF CALIFORNIA**

13 REBECCA MEDINA, individually and on  
 14 behalf of all others similarly situated,

15 Plaintiff,

17 v.

18 CHANGE HEALTHCARE INC., OPTUM,  
 19 INC. and UNITEDHEALTH GROUP  
 20 INCORPORATED,

21 Defendants.

Case No. \_\_\_\_\_

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

1 Plaintiff Rebecca Medina, individually and on behalf of all others similarly situated, alleges  
2 the following based on her personal experience and her counsel’s investigation:

3 **INTRODUCTION**

4 1. Plaintiff brings this proposed class action lawsuit against Defendants Change  
5 Healthcare Inc., Optum, Inc., and UnitedHealth Group Incorporated (“Defendants”) for their  
6 negligent failure to protect Plaintiff and Class members’ confidential health and personal  
7 identifying information from ALPHV/Blackcat (“Blackcat”), a well-known group of  
8 cybercriminals. Defendants are key players in the U.S. health industry and together, they process  
9 50% of all medical claims in the United States through a pervasive network of approximately  
10 900,000 physicians, 118,000 dentists, 33,000 pharmacies, 5,500 hospitals and 600 laboratories.

11 2. On or around February 21, 2024, Blackcat infiltrated Defendants’ information  
12 technology networks and then stole for ransom the confidential personal identifying information  
13 (“PII”) and personal health information (“PHI”) of millions of patients across the United States.  
14 The stolen information includes names, phone numbers, addresses, Social Security Numbers,  
15 medical and dental records, insurance records, and claims and payment information, among other  
16 things. Blackcat also encrypted portions of Defendants’ network, essentially locking them out.

17 3. In response to the security breach, Defendants immediately took their network systems  
18 offline—and three weeks later—they remain offline. According to a statement from Change  
19 Healthcare, the systems “will remain offline until [they] can be turned back on safely.”<sup>1</sup>

20 4. The security breach and shutdown has crippled the U.S. healthcare system and has  
21 negatively impacted patients, hospital systems, physicians, clinical social workers, and both  
22 private and government-owned pharmacies. Medical providers cannot verify insurance coverage  
23 for patient treatment and procedures or receive reimbursement for services rendered. According to  
24  
25  
26

27 \_\_\_\_\_  
28 <sup>1</sup> See <https://www.usnews.com/news/health-news/articles/2024-03-04/explainer-what-to-know-about-the-change-healthcare-cyberattack> (last visited March 4, 2024).

1 an estimate from First Health Advisory, a digital risk assurance firm, the Data Breach “is costing  
2 some providers over \$100 million a day.”<sup>2</sup>

3 5. But perhaps the most negatively impacted are patients who cannot timely access  
4 medical treatment, including much needed prescription drugs, and now face a significant and  
5 increased risk of identity theft. According to Rick Pollack, President and CEO of the American  
6 Hospital Association (“AHA”), the Data Breach is the “most serious incident of its kind leveled  
7 against a U.S. healthcare organization.”

8 6. Blackcat is known to target organizations with high-value data, such as PHI, and once  
9 inside their networks, Blackcat encrypts the organization’s data, networks, and servers to block the  
10 organization from access until a ransom is paid in exchange for a key that releases the data. But  
11 even when Blackcat’s demands are met, it may publish the stolen data on the Dark Web. Blackcat  
12 affiliates claim they still have the stolen data although a ransom has allegedly been paid by  
13 UnitedHealth Group.

14 7. The U.S. government has warned that Blackhat has hit at least 70 organizations since  
15 December 2023, a majority of them healthcare organizations.

16 8. Plaintiff, individually and on behalf of all others similarly situated, alleges claims for  
17 negligence, negligence *per se*, unjust enrichment, violations of California’s Unfair Competition  
18 Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*, and violations of California’s Confidentiality of  
19 Medical Information Act, Cal. Civ. Code § 56, *et seq.* against Defendants and seeks all available  
20 monetary and equitable relief.

21 **PARTIES**

22 9. Rebecca Medina is a resident and citizen of Sutter Creek, California in Amador County.

23 10. Defendant Change Healthcare Inc. is a publicly traded company headquartered in  
24 Nashville, Tennessee and incorporated in Delaware. It became a subsidiary of UnitedHealth Group  
25 Incorporated in 2022 and merged with OptumInSight that same year.

26 11. Defendant Optum, Inc. (“Optum”) is headquartered in Eden Prairie, Minnesota

27 \_\_\_\_\_  
28 <sup>2</sup> *Id.*

1 and is incorporated in Delaware. Optum provides healthcare technology, analytics and services,  
2 primarily to United Healthcare, the largest commercial health insurer in the United States.

3 12. Defendant UnitedHealth Group Incorporated (“United”) is one of the largest publicly  
4 traded companies by revenue and is headquartered in Minnetonka, Minnesota and incorporated in  
5 Delaware. United is a vertically integrated enterprise with several wholly owned subsidiaries,  
6 including Change Healthcare and Optum.

7 **JURISDICTION AND VENUE**

8 13. This Court has jurisdiction over this action under the Class Action Fairness  
9 Act, 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated  
10 claims of the individual class members exceed the sum or value of \$5,000,000, exclusive of  
11 interests and costs, and this is a class action in which one or more members of the proposed class,  
12 including Plaintiff, are citizens of a state different from Defendants. The Court has supplemental  
13 jurisdiction over the alleged state law claims under 28 U.S.C. § 1367 because they form part of the  
14 same case or controversy.

15 14. This Court may exercise jurisdiction over Defendants because they are registered to  
16 conduct business in California; have sufficient minimum contacts in California; and intentionally  
17 avail themselves of the markets within California through the promotion, sale, marketing, and  
18 distribution of the Class Vehicles, thus rendering the exercise of jurisdiction by this Court proper  
19 and necessary.

20 15. Venue is proper in this District under 28 U.S.C. § 1391 because Plaintiff resides in  
21 this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims  
22 occurred in this District.

23 **FACTUAL ALLEGATIONS**

24 **Background**

25 16. Change Healthcare is a healthcare technology company that offers health care  
26 providers, pharmacies, and insurance companies claims and reimbursement management, billing  
27 solutions, and prescription processing. It is one of the largest processors of prescription medicines  
28 and handles the billing for thousands of pharmacies across the country.

1 17. According to the Change Healthcare website, its “extensive network, innovative  
2 technology, and expertise inspire a stronger, better coordinated, increasingly collaborative, and  
3 more efficient healthcare system.” It bills itself as a “trusted partner for organizations committed  
4 to improving the healthcare system through technology.”

5 18. Change Healthcare also represents to providers that its “advanced technology and  
6 services helps [them] enhance patient engagement and access, improve outcomes, drive revenue  
7 performance, and improve operational efficiency.” Change Healthcare represents to payers that its  
8 “advanced technology solutions and services help payers achieve their priorities across the  
9 member journey.” Change Healthcare promises its partners that its “advanced technology solutions  
10 empower our partners to achieve their strategic business objectives and meet their customers’  
11 needs.” And it assures patients that its “solutions streamline the engagement, care, and payment  
12 experience to improve the patient journey.”

13 19. Change Healthcare processes 15 billion healthcare transactions annually and has access  
14 to one of every three U.S. patient records through its clinical connectivity solutions.

15 20. Previously, Change Healthcare was an independent company that was not owned by  
16 any particular healthcare provider or insurer. In 2021, United proposed a deal to acquire Change  
17 Healthcare and merge it with Optum.

18 21. Melinda Reid Hatton, AHA Vice President and General Counsel, voiced concerns about  
19 the proposed deal and wrote to the DOJ asking it to investigate. In the letter to the DOJ, Ms. Hatton  
20 wrote, “The proposed acquisition would produce a massive consolidation of competitively  
21 sensitive healthcare data and shift such data from Change Healthcare, a neutral third party, to  
22 Optum.”<sup>3</sup>

23 22. The DOJ did investigate and filed a complaint to stop United’s transaction. In its  
24 complaint, the DOJ described Change Healthcare as a technology company that operates “the  
25 nation’s largest electronic data interchange (EDI) clearinghouse, which transmits data between  
26

27 <sup>3</sup> See <https://www.darkdaily.com/2021/04/07/aha-expresses-opposition-to-merger-between-unitedhealth-groups-optuminsight-and-change-healthcare-doj-agrees-to-look-into-the-13b-deal/>  
28 (last visited March 4, 2024).

1 healthcare providers and insurers, allowing them to exchange insurance claims, remittances, and  
2 other healthcare-related transactions . . . It has access to a vast trove of competitively sensitive  
3 claims data that flows through its EDI clearinghouse—over a decade’s worth of historic data as  
4 well as billions of new claims each year.”

5 23. Moreover, according to the DOJ, “50 percent of all medical claims in the United States  
6 pass through Change’s EDI clearinghouse. Change’s self-described ‘pervasive network  
7 connectivity,’ including approximately ‘900,000 physicians, 118,000 dentists, 33,000 pharmacies,  
8 5,500 hospitals and 600 laboratories,’ means that even when United’s health insurer rivals choose  
9 not to be a Change customer, health insurers have no choice but to have their claims data pass  
10 through Change’s EDI clearinghouse. Not only does Change process vast amounts of  
11 competitively sensitive claims data, but it also has secured ‘unfettered’ rights to use over 60 percent  
12 of this data for its own business purposes including, for example, using claims data for healthcare  
13 analytics. Additionally, through its claims editing product, Change has access to the proprietary  
14 plan and payment rules for all of United’s most significant health insurance competitors.”

15 24. The DOJ, however, lost its challenge to United’s acquisition of Change Healthcare after  
16 a district judge ruled in United’s favor and chose not to appeal.

17 **Defendants Targeted for Their Treasure Trove of Health Data**

18 25. On or around February 21, 2024, United discovered a security breach of Change  
19 Healthcare’s information technology network (hereinafter, “Data Breach”). According to United’s  
20 filing with the U.S. Securities and Exchange Commission, the company immediately took the  
21 impacted systems offline. The shutdown has disrupted the operations of thousands of hospitals,  
22 healthcare providers, and pharmacies across the United States.

23 26. In a public statement, Defendants stated:

24 Change Healthcare can confirm we are experiencing cyber security issues  
25 perpetrated by a cybercrime threat actor who has represented itself to us as  
ALPHV/Blackcat.

26 Our experts are working to address the matter and we are working closely with law  
27 enforcement and leading third-party consultants, Mandiant and Palo Alto Network,  
28 on this attack against Change Healthcare’s systems. We are actively working to  
understand the impact to members, patients, and consultants.

1 Patient care is our top priority, and we have multiple workarounds to ensure people  
2 have access to the medications and the care they need. Based on our ongoing  
3 investigation, there's no indication that Optum, UnitedHealthcare and  
4 UnitedHealthcare Group systems have been affected by this issue.

5 We are working on multiple approaches to restore the impacted environment and  
6 continue to be proactive and aggressive with all our systems, and if we suspect any  
7 issue with the system, we will immediately take action.<sup>4</sup>

8 27. Upon the public announcement, the AHA issued a security advisory on February 22,  
9 2024, stating:

10 Due to the sector wide presence and the concentration of mission critical services  
11 provided by Optum, the reported interruption could have significant cascading and  
12 disruptive effects on revenue cycle, certain health care technologies and clinical  
13 authorizations provided by Optum across the health care sector. Based upon the  
14 statements from Change Healthcare that they became aware of an "outside threat"  
15 and disconnected "in the interest of protecting our partners and patients," **we  
16 recommend that all health care organizations that were disrupted or are  
17 potentially exposed by this incident consider disconnection from Optum until  
18 it is independently deemed safe to reconnect to Optum.** It also is recommended  
19 that organizations which utilize Optum's services prepare related downtime  
20 procedures and contingency plans should Optum's services remain unavailable for  
21 an extended period.<sup>5</sup>

22 (emphasis in original).

23 28. Two days later, AHA issued another security advisory notifying members and the  
24 public that "**Change Healthcare has not provided a specific timeframe for which recovery of  
25 the impacted applications is expected**" (emphasis in original).<sup>6</sup> The AHA also recognized that  
26 hospitals and health systems "may be experiencing challenges with obtaining care authorizations  
27  
28

---

<sup>4</sup> See <https://status.changehealthcare.com/incidents/hqpjz25fn3n7> (last visited March 4, 2024)

<sup>5</sup> See <https://www.aha.org/advisory/2024-02-22-unitedhealth-groups-change-healthcare-experiencing-cyberattack-could-impact-health-care-providers-and> (last visited March 4, 2024).

<sup>6</sup> See <https://www.aha.org/2024-02-24-update-unitedhealth-groups-change-healthcares-continued-cyberattack-impacting-health-care-providers> (last visited March 4, 2024).

1 for their patients, as well as delays in payment.”<sup>7</sup> It stated that it was in communication with the  
2 Department of Health and Human Services, including the Centers for Medicare & Medicaid  
3 Services, about “options to support patients’ timely access to care and provide temporary financial  
4 support to providers. We also are having these discussions with Optum. We will provide more  
5 information as it becomes available.”<sup>8</sup>

6 29. On February 23, 2024, the AHA called the Data Breach a “threat to life,” and in a letter  
7 to Health and Human Services, the AHA stated that while the full scope was “unknown,” the AHA  
8 expected impacts to be far-reaching given Change Healthcare’s national presence.<sup>9</sup> The AHA also  
9 explained how the incident has affected healthcare providers in terms of being unable to collect  
10 revenue. “[W]ithout this critical revenue source, hospitals and health systems may be unable to  
11 pay salaries for clinicians and other members of the care team, acquire necessary medicines and  
12 supplies, and pay for mission critical contract work in areas such as physical security, dietary and  
13 environmental services,” the AHA stated.<sup>10</sup> “In addition, replacing previously electronic processes  
14 with manual processes will add considerable administrative costs on providers, as well as divert  
15 team members from other tasks. It is particularly concerning that while Change Healthcare’s  
16 systems remain disconnected, it and its parent entities benefit financially, including by accruing  
17 interest on potentially billions of dollars that belong to health care providers.”<sup>11</sup>

18 30. Antitrust experts have opined that the Data Breach shows why placing “one  
19 conglomerate at the center of multiple health care functions is inherently risky.”<sup>12</sup>

20 \_\_\_\_\_  
21 <sup>7</sup> *Id.*

22 <sup>8</sup> *Id.*

23 <sup>9</sup> See [https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-](https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack)  
24 [healthcare-cyberattack](https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack) (last visited March 4, 2024).

25 <sup>10</sup> *Id.*

26 <sup>11</sup> *Id.*

27 <sup>12</sup> See [https://www.statnews.com/2024/02/27/change-healthcare-cyber-attack-reveals-](https://www.statnews.com/2024/02/27/change-healthcare-cyber-attack-reveals-consolidation-risks/)  
28 [consolidation-risks/](https://www.statnews.com/2024/02/27/change-healthcare-cyber-attack-reveals-consolidation-risks/) (last visited March 4, 2024).



**The Change Healthcare Data Breach Cripples the Healthcare Industry**

31. The Data Breach at Change Healthcare has had reverberations across the U.S. healthcare industry that continue today. The most negatively impacted are patients who are having trouble accessing their prescriptions and healthcare and now face an increased risk of identity theft.

32. One week after the Data Breach, hospitals, healthcare providers, and pharmacies across the U.S. have continued to report that they are unable to process and fill prescriptions through patients’ insurance.

33. U.S. military insurance provider, Tricare, said that the Data Breach was “impacting all military pharmacies worldwide and some retail pharmacies nationally.”<sup>13</sup>

34. In a post on X, the Naval Hospital in Camp Pendleton, California said it was unable to process any prescriptions.<sup>14</sup> “Due to an ongoing enterprise-wide issue, all Camp Pendleton and associated pharmacies are unable to process any prescription claims,” Camp Pendleton said.<sup>15</sup> “As a result, we are only able to assist patients with emergency and urgent prescriptions from hospital providers at this time.”<sup>16</sup>

35. In a Facebook post, Evans Army Community Hospital similarly reported problems: “This outage is impacting dispensing of pharmacy prescriptions – resulting in delays in processing and in some cases, inability to process. Refills have also been impacted.”<sup>17</sup>

---

<sup>13</sup>See <https://tcrn.ch/3Tg4jsV> (last visited March 4, 2024).

<sup>14</sup> See <https://www.cnn.com/2024/02/22/tech/us-pharmacies-face-delays-filling-prescriptions-because-of-cyberattack/index.html> (last visited March 4, 2024).

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

1 36. GoodRx, which offers discounted prescriptions, also said on X: “We apologize for  
2 any outages you have been experiencing while at the pharmacy . . . Unfortunately, the issue  
3 is an external one impacting both GoodRx and a multitude of providers.”<sup>18</sup>

4 37. Large pharmacy chains like CVS and Walgreens have also reported disruptions as  
5 well as smaller ones like Moffet Drug in Norton, Kansas.<sup>19</sup>

6 38. Armish Patel, a pharmacist in Dallas, Texas, told CBS: “So I mean we've seen a  
7 lot of claims coming through as a rejected claim, where obviously the insurance provider are  
8 not able to pay because of this attack . . . Elderly patients that have a fixed income, and  
9 they're trying to get their medicine...unfortunately there's no way around it at this point.”<sup>20</sup>

10 39. One consumer, Cary Brazeman, told CNBC that he tried to pick up a prescription  
11 at Vons pharmacy in Palm Springs after seeing his dermatologist but was told by the  
12 pharmacy that it had not received his prescription and that even if it had, it would not have  
13 been able to process it with his insurance. Brazeman asked what he was supposed to do, and  
14 was told by the pharmacy, “We don’t know.” Brazeman told CNBC, “I’m mobile, so I can  
15 make the rounds if necessary, and I can pay cash if necessary, but there’s a lot of people who  
16 cannot.”<sup>21</sup>

17 40. The fallout from the Data Breach has also impacted medical care providers, both large  
18 and small.

19  
20  
21  
22 \_\_\_\_\_  
23 <sup>18</sup> *Id.*

24 <sup>19</sup> See <https://www.cnn.com/2024/02/22/tech/us-pharmacies-face-delays-filling-prescriptions-because-of-cyberattack/index.html> (last visited March 4, 2024).

25 <sup>20</sup> See <https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/> (last visited March 4, 2024).

26  
27 <sup>21</sup> See <https://www.cnn.com/2024/02/27/unitedhealths-change-healthcare-cyberattack-outages-continue-pharmacies-deploy-workarounds.html> (last visited March 4, 2024).

1 41. A majority of Nebraska hospitals have also been unable to verify patient insurance,  
2 process billing, or provide accurate cost estimates, according to Nebraska television outlet KLKN-  
3 TV.<sup>22</sup> When insurance cannot be verified, treatment is delayed.

4 42. Similarly, independent medical practitioners reported to CNBC that they also have been  
5 unable to verify patients' eligibility for patients or electronically fill prescriptions, which has  
6 created a headache and more clerical work that is overwhelming and time consuming.<sup>23</sup>

7 43. Moreover, some medical practices, especially smaller ones and mid-sized offices, rely  
8 on cash flow from claims reimbursements that are not being processed. Dr. Purvi Parikh told  
9 CNBC that her practice has not been paid from insurers for her patients' visits, which creates  
10 problems for paying operational expenses like medical supplies and payroll.<sup>24</sup> Dr. Parikh said there  
11 were no immediate workarounds and that it could take weeks to change to a new platform.<sup>25</sup>

12 44. Licensed clinical social worker Jenna Wolfson reported that she has been unable to  
13 receive any payments due to the Change Healthcare Data Breach and that many of her colleagues  
14 are facing the same problems.<sup>26</sup> According to Wolfson, "There are people right now that might not  
15 see payment on the work that they're doing today for months, and they still have an entire practice  
16 to keep above water."<sup>27</sup>

17  
18  
19  
20  
21 <sup>22</sup> See <https://tcrn.ch/3Tg4jsV> (last visited March 4, 2024).

22 <sup>23</sup> See <https://www.nbcnews.com/news/us-news/outages-change-healthcare-cyberattack-causing-financial-mess-doctors-rcna141321> (last visited March 4, 2024).

23  
24 <sup>24</sup> *Id.*

25 <sup>25</sup> *Id.*

26 <sup>26</sup> See <https://healthitsecurity.com/features/understanding-the-impact-of-the-change-healthcare-cyberattack-on-providers> (last visited March 4, 2024).

27  
28 <sup>27</sup> *Id.*

**The Data Breach has Also Placed the Confidential Health and Personal Identifying Information of Patients at Risk**

45. UnitedHealthcare Group initially claimed that a nation-state actor was responsible for the Data Breach. Blackcat, however, claimed responsibility and stated on its dark web leak site that it had stolen the confidential health and personal identifying information relating to millions of Americans.

46. Specifically, Blackcat said it gained access to 6TB of data, including medical records, and payment and claims information containing personally identifiable information like names, contact information such as phone numbers and email addresses, and Social Security Numbers.

47. Blackcat also claims to have Change Healthcare’s source code and confidential and sensitive information of CVS Caremark, Metlife, Health Net, Federal Medicare, and Tricare.

48. Below is the statement that Blackcat issued regarding the cyberattack, indicating that the group has reviewed a substantial amount of confidential medical and personal identifying information:

Change Healthcare - Optum - UnitedHealth

2/28/2024, 4:19:59 PM

UnitedHealth has announced that the attack is “strictly related” to Change Healthcare only and it was initially attributed to a nation state actor.

Two lies in one sentence.

Only after threatning [sic] them to announce it was us, they started telling a different story.

It is true that the attack is centered at Change Healthcare production and corporate networks, but why is the damage extremely high? Change Healthcare production servers process extremely sensitive data to all of UnitedHealth clients that rely on Change Healthcare technology solutions. Meaning thousands of healthcare providers, insurance providers, pharmacies, etc . . .

Also, being inside a production network one can imagine the amount of critical and sensitive data that can be found.

We were able to exfiltrate to be exact more than 6 TB of highly selective data. The data relates to all Change Health clients that have sensitive data being processed by the company.

1 The list of affected Change Health partners that we have sensitive data for is  
2 actually huge with names such as:

- 3 - Medicare
- 4 - Tricare
- 5 - CVS-CareMark
- 6 - Loomis
- 7 - Davis Vision
- 8 - Health Net
- 9 - MetLife
- 10 - Teachers Health Trust
- 11 - Tens of insurance companies and others

11 Anyone with some decent critical thinking will understand what damage can be  
12 done with such intimate data on the affected clients of UnitedHealth/UnitedHealth  
13 solutions as well, beyond simple scamming/spamming.

14 After 8 days and Change Health have [sic] still not restored its operations and chose  
15 to play a very risky game hence our announcement today.

16 So for everyone, both those affected and fellow associates. [sic] to understand what  
17 is at stake our exfiltrated data includes millions of:

- 18 - active US military/navy personnel PII
- 19 - medical records
- 20 - dental records
- 21 - payments information
- 22 - Claims information
- 23 - Patients PII including Phone numbers/addresses/SSN/emails/etc ...
- 24 - 3000+ source code files for Change Health solutions (for source-code review  
25 gents out there)
- 26 - Insurance records
- 27 - many many more

28 UnitedHealth you are walking on a very thin line be careful you just might fall over.

PS: For all those cyber intelligence so called expert . . . we did not use ConnectWise  
exploit as our initial access so you should base your reports you tell people on actual  
facts not kiddi [sic] speculations.

1 49. On February 28, 2024, United confirmed that the Data Breach was perpetrated by  
2 Blackcat, which has a history of targeting organizations in the healthcare industry.

3 50. As a result of the Data Breach, Plaintiff and the proposed Class have not only lost their  
4 privacy, but they are at a significant and increased risk of identity theft.

5 51. The FTC defines identity theft as “a fraud committed or attempted using the  
6 identifying information of another person without authority.” 17 C.F.R. § 248.201 (2013). The  
7 FTC describes “identifying information” as “any name or number that may be used, alone or in  
8 conjunction with any other information, to identify a specific person,” including, among other  
9 things, “[n]ame, Social Security number, date of birth, official State or government issued driver's  
10 license or identification number, alien registration number, government passport number, employer  
11 or taxpayer identification number.” *Id.*

12 52. The United States Government Accountability Office noted in a June 2007  
13 report on data breaches (“GAO Report”) that identity thieves use identifying data such as Social  
14 Security Numbers to open financial accounts, receive government benefits and incur charges and  
15 credit in a person's name.<sup>28</sup> As the GAO Report states, this type of identity theft is the most harmful  
16 because it often takes some time for the victim to become aware of the theft, and the theft can  
17 impact the victim's credit rating adversely.

18 53. Accordingly, identity theft victims must spend countless hours and large amounts of  
19 money repairing the impact to their credit.<sup>29</sup>

20 54. PII is such a valuable commodity to identity thieves that once the information has been  
21  
22

---

23 <sup>28</sup> See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft  
24 is Limited; However, the Full Extent Is Unknown (June 2007), United States Government  
25 Accountability Office, available at <https://www.gao.gov/new.items/d07737.pdf> (last accessed  
January 15, 2020).

26 <sup>29</sup> Guide for Assisting Identity Theft Victims, Federal Trade Commission, 4 (September 2013),  
27 available at <http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf>  
28 (last accessed January 15, 2020).

1 compromised, criminals often trade the information on the dark web for years. According to the  
2 GAO Report:

3 [L]aw enforcement officials told us that in some cases, stolen data may be held for  
4 up to a year or more before being used to commit identity theft. Further, once stolen  
5 data have been sold or posted on the Web, fraudulent use of that information may  
6 continue for years. As a result, studies that attempt to measure the harm resulting  
7 from data breaches cannot necessarily rule out all future harm.<sup>30</sup>

8 55. A study by Experian found that the “average total cost” of medical identity  
9 theft is “about \$20,000” per incident, and that a majority of victims of medical identity theft were  
10 forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.<sup>46</sup>

11 56. Indeed, data breaches and identity theft have a crippling effect on individuals and  
12 detrimentally impact the entire economy as a whole.

13 57. For all of the above reasons, Plaintiff and the Class members have suffered  
14 harm and there is a substantial risk of injury to them that is imminent and concrete and that will  
15 continue for years to come.

16 **The Data Breach was a Foreseeable Risk of Which**  
17 **Defendants were on Notice and Could Have Prevented**

18 58. The healthcare industry is the most targeted industry by cybercriminals; cyberattacks  
19 have doubled from 2016 to 2021. As a result, the personal health information of approximately 42  
20 million patients has been exposed.<sup>31</sup>

21 59. Identity thieves and cybercriminals have targeted the medical industry in the last  
22 several years given the treasure trove of ultra-sensitive personal data stored on their systems. The  
23 medical industry is rife with examples of cybercriminals targeting healthcare providers.

24  
25 \_\_\_\_\_  
26 <sup>30</sup> GAO Report at 29.

27 <sup>31</sup> See  
28 <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9856685/#:~:text=In%20this%20cohort%20study%20of,of%20nearly%2042%20million%20patients> (last visited March 4, 2024).

1 60. In addition, cyberattacks at medical facilities wreak havoc on patients' lives because  
2 they disrupt the medical treatments needed, resulting in delays or cancellations in receiving  
3 medical care. Such attacks cause loss of access to patient medical records, including charts, x-rays,  
4 and other information needed to treat patients.

5 61. The Department of Health and Human Services in 2017 released a ransomware fact  
6 sheet advising entities covered by HIPAA that “[w]hen electronic protected health information  
7 (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI  
8 encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession  
9 or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy  
10 Rule.”

11 62. Under the HIPAA Privacy Rules, a breach is defined as, “. . . the acquisition, access,  
12 use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which  
13 compromises the security or privacy of the PHI.” Accordingly, attacks like the one at issue are  
14 considered a breach under the HIPAA Rules because there was an access of PHI not permitted  
15 under the HIPAA Privacy Rule.

16 63. A ransomware attack is also considered a “Security Incident” under HIPAA.  
17 Under the HIPAA Rules, a “Security Incident” is defined as “the attempted or successful  
18 unauthorized access, use, disclosure, modification, or destruction of information or interference  
19 with system operations in an information system.” According to the Department of Health and  
20 Human Services, “[t]he presence of ransomware (or any malware) on a covered entity’s or business  
21 associate's computer systems is a security incident under the HIPAA Security Rule.”

22 64. As early as 2014, the FBI alerted healthcare stakeholders that they were the target of  
23 hackers, stating “[t]he FBI has observed malicious actors targeting healthcare related systems,  
24 perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally  
25 Identifiable Information (PII).”

26 65. Data Breaches can be prevented. Approximately 80% of ransomware is delivered  
27 through email phishing attacks. Other means to deliver ransomware is through brute force attacks  
28 on open remote desktop protocol ports. To prevent ransomware attacks, organizations must provide



1 training to its employees for the handling of suspicious emails. They can also disable macros, avoid  
2 storing passwords in plain text, and perform hunts and search for suspicious behavior in their  
3 networks, among other things.

4 66. Accordingly, Defendants knew, given the vast amount of PII and PHI they  
5 acquire, manage and maintain, that they were a target of security threats, and therefore understood  
6 the risks posed by their insecure data security practices and systems. Defendants' failure to heed  
7 warnings and to otherwise maintain adequate security practices resulted in this ransomware attack.

8 **Defendants, at all Relevant Times, had a Duty to Plaintiff and Class Members to Properly**  
9 **Secure Their PII and PHI**

10 67. Defendants, at all relevant times, had a duty to Plaintiff and Class members to properly  
11 secure their PII and PHI, encrypt and maintain such information using industry standard methods,  
12 utilize available technology to defend their systems from invasion, act reasonably to prevent  
13 foreseeable harms to Plaintiff and Class members, and promptly notify patients when Defendants  
14 became aware that patients' PII and PHI was compromised.

15 68. Defendants' duty to use reasonable security measures arose as a result of the special  
16 relationship that existed between them, on the one hand, and Plaintiff and the other Class members,  
17 on the other hand. The special relationship arose because Plaintiff and the members of the Class  
18 entrusted Defendants (or their providers who entrusted Defendants) with their PII and PHI as part  
19 of receiving or paying for medical services and prescription drugs. Defendants had the resources  
20 necessary to prevent the Data Breach but neglected to adequately invest in security measures,  
21 despite their obligations to protect such information. Accordingly, Defendants breached its  
22 common law, statutory and other owed duties to Plaintiff and Class members.

23 69. Defendants' duty to use reasonable security measures also arose under HIPAA. Under  
24 HIPAA, Defendants were required to "reasonably protect" PHI from "any intentional or  
25 unintentional use or disclosure" and to "have in place appropriate administrative, technical, and  
26 physical safeguards to protect the privacy of protected health information." 45 C.F.R. §  
27 164.530(c)(1). Plaintiff's and Class members' sensitive information that was compromised in the  
28

1 Data Breach includes PHI, such as provider names, dates of service, medical billing information  
2 and potentially other “protected health information” within the meaning of HIPAA.

3 70. Under HIPPA, Defendants were also required to do the following:

- 4 • Ensure the confidentiality and integrity of electronic PHI they created, received,  
5 maintained, and/or transmitted. 45 C.F.R. § 164.306(a)(1);
- 6 • Implement technical policies and procedures for electronic information systems  
7 that maintain electronic PHI to allow access only to those persons or software  
8 programs that have been granted access rights. 45 C.F.R. § 164.312(a)(1);
- 9 • Implement policies and procedures to prevent detect, contain, and correct  
10 security violations. 45 C.F.R. § 164.308(a)(1)(i);
- 11 • Implement procedures to review records of information system activity  
12 regularly, such as audit logs, access reports, and security incident tracking  
13 reports. 45 C.F.R. § 164.308(a)(1)(ii)(D);
- 14 • Protect against reasonably anticipated threats or hazards to the security or  
15 integrity of electronic PHI. 45 C.F.R. § 164.306(a)(2);
- 16 • Protect against reasonably anticipated uses or disclosures of electronic PHI that  
17 are not permitted under the privacy rules regarding individually identifiable  
18 health information. 45 C.F.R. § 164.306(a)(3);
- 19 • Ensure compliance with HIPAA security standard rules by its workforces. 45  
20 C.F.R. § 164.306(a)(4);
- 21 • Train all members of its workforces effectively on the policies and procedures  
22 regarding PHI as necessary and appropriate for the members of its workforces  
23 to carry out their functions and to maintain security of PHI. 45 C.F.R. §  
24 164.530(b); and/or
- 25 • Render the electronic PHI it maintained unusable, unreadable, or  
26 indecipherable to unauthorized individuals, as it had not encrypted the  
27 electronic PHI as specified in the HIPAA Security Rule by “the use of an  
28 algorithmic process to transform data into a form in which there is a low

1 probability of assigning meaning without use of a confidential process or key”  
2 (45 CFR 164.304 definition of encryption).

3 71. Defendants’ duty to use reasonable security measures also arose under Section 5 of the  
4 Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting  
5 commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use  
6 reasonable measures to protect confidential data by entities like Defendant.

7 72. The Data Breach was a direct and proximate result of Defendants’ failure to: (1)  
8 properly safeguard and protect Plaintiffs’ and Class members’ PII and PHI from unauthorized  
9 access, use, and disclosure, as required by various state and federal regulations, industry practices,  
10 and common law; (2) establish and implement appropriate safeguards to ensure the security and  
11 confidentiality of Plaintiffs’ and Class members’ PII and PHI; and (3) protect against reasonably  
12 foreseeable threats to the security or integrity of such information.

13 **Plaintiff’s Experience**

14 73. Plaintiff Rebecca Medina has a medical condition that requires that she take certain  
15 medications every day. She uses Lone Pharmacy to fill her prescriptions.

16 74. On March 1, 2024, Plaintiff tried to fill a prescription but was told by Lone Pharmacy  
17 that the systems were down due to a cyberattack and that it did not know when they would be back  
18 up. Plaintiff had to pay for her prescription out of pocket.

19 75. Plaintiff Medina has spent time and efforts researching the data breach and reviewing  
20 her financial information to determine if there has been unauthorized activity to her accounts and  
21 will perform these activities for the foreseeable future. In addition to not being able to timely obtain  
22 her necessary medications, Plaintiff Medina has suffered emotional distress due to the Data Breach  
23 and concerns that her PII and PHI is in the hands of cybercriminals and can be ransomed again  
24 and otherwise used for identity theft.

25 **CLASS ACTION ALLEGATIONS**

26 76. Plaintiff brings this action individually and on behalf of all other persons similarly  
27 situated (the “Nationwide Class”) pursuant to the Federal Rule of Civil Procedure 23(b)(2), (b)(3),  
28 and (c)(4).

1 77. The Nationwide Class is initially defined as follows: All persons residing in the United  
2 States and whose PII and PHI was compromised in the Data Breach announced by Defendants on  
3 or around February 21, 2024.

4 78. Additionally, pursuant to the Federal Rule of Civil Procedure 23(b)(2), (b)(3), and  
5 (c)(4), Plaintiff brings this action on behalf of the following California Class initially defined as:  
6 All persons who reside in the state of California and whose PII and PHI was compromised in the  
7 Data Breach announced by Defendants on or around February 21, 2024.

8 79. The Nationwide Class and the California Class are referred to herein as “Class,” unless  
9 otherwise stated.

10 80. Excluded from the proposed Class are: Defendants, any entity in which Defendants  
11 have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well  
12 as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and  
13 assigns of Defendants; and judicial officers to whom this case is assigned and their immediate  
14 family members.

15 81. Plaintiffs reserve the right to re-define the Class definition after conducting discovery.

16 82. Numerosity (Fed. R. Civ. P. 23(a)(1)). The Class members are so numerous that joinder  
17 of all members is impracticable. Based on information and belief, the Class includes millions of  
18 patients who had their PII and PHI compromised. The parties will be able to identify the exact size  
19 of the Class through discovery and Defendants’ records.

20 83. Commonality and Predominance (Fed. R. Civ. P. 23(a)(2); 23(b)(3)). Common  
21 questions of law and fact exist for each of the claims and predominate over questions affecting  
22 only individual members of the Class. Questions common to the Class include, but not limited to  
23 the following:

- 24 a. Whether Defendants had a legal duty to implement and maintain reasonable  
25 security procedures and practices for the protection of Plaintiff’s and Class  
26 members’ PII and PHI;

- b. Whether Defendants breached their legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiff's and Class members' PII and PHI;
- c. Whether Defendants' conduct, practices, actions, and omissions, resulted in or was the proximate cause of the Data Breach, resulting in the loss of PII and PHI of Plaintiff and Class members;
- d. Whether Defendants had a legal duty to provide timely and accurate notice of the data breach to Plaintiff and Class members;
- e. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class members;
- f. Whether and when Defendants knew or should have known that their systems were vulnerable to attack;
- g. Whether Defendants violated the Unfair Competition Law;
- h. Whether Defendants violated the Confidentiality of Medical Information Act;
- i. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of their PII and PHI; and
- j. Whether Plaintiff and Class members are entitled to relief, including damages and equitable relief.

84. **Typicality (Fed. R. Civ. P. 23(a)(3)).** Pursuant to Rule 23(a)(3), Plaintiff's claims are typical of the claims of the Class members. Plaintiff, like all Class members, had her PII and PHI compromised in the Data Breach and is at an increased risk of harm, including identity theft.

85. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)).** Pursuant to Rule 23(a)(4), Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Plaintiff has no interest antagonistic to, or in conflict with, the interests of the Class members. Plaintiff has retained counsel experienced in prosecuting class actions and data breach cases.

1           **86. Superiority (Fed. R. Civ. P. 23(b)(3).** Pursuant to Rule 23(b)(3), a class  
2 action is superior to individual adjudications of this controversy. Litigation is not economically  
3 feasible for individual Class members because the amount of monetary relief available to  
4 individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation  
5 could yield inconsistent or contradictory judgments and increase the delay and expense to all  
6 parties and the court system. A class action presents fewer management difficulties and provides  
7 the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single  
8 court.

9           **87. Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final**  
10 **Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)).** In the alternative, this action  
11 may properly be maintained as a class action, because:

- 12           a. the prosecution of separate actions by individual members of the Class would create  
13           a risk of inconsistent or varying adjudication with respect to individual Class  
14           members which would establish incompatible standards of conduct for Defendant;  
15           or  
16           b. the prosecution of separate actions by individual Class members would create a risk  
17           of adjudications with respect to individual Class members which would, as a  
18           practical matter, be dispositive of the interests of other Class members not parties  
19           to the adjudications, or substantially impair or impede their ability to protect their  
20           interests; or  
21           c. Defendants have acted or refused to act on grounds generally applicable to the  
22           Class, thereby making appropriate final injunctive or corresponding declaratory  
23           relief with respect to the Class as a whole.

24           **88. Issue Certification (Fed. R. Civ. P. 23(c)(4).** In the alternative, the common questions  
25 of fact and law, set forth in Paragraph 81, are appropriate for issue certification on behalf of the  
26 proposed Class.

27 //

1                                    **CAUSES OF ACTION**  
 2    **COUNT I**  
 3    **NEGLIGENCE**  
**(On Behalf of Plaintiff and the Nationwide Class)**

4                      89. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth  
 5 herein.

6                      90. Defendants had (and continue to have) a duty to Plaintiff and Class members to exercise  
 7 reasonable care in safeguarding and protecting their PII and PHI. Defendants also had (and  
 8 continue to have) a duty to use ordinary care in activities from which harm might be reasonably  
 9 anticipated (such as in the storage and protection of PII and PHI within their possession, custody  
 10 and control).

11                     91. Defendants' duty to use reasonable security measures arose as a result of  
 12 the special relationship that existed between them and Plaintiff and Class members, which is  
 13 recognized by laws including but not limited to HIPAA. Only Defendants were in a position to  
 14 ensure that their systems were sufficient to protect against the harm to Plaintiff and the Class  
 15 members from a data breach.

16                     92. Defendants violated these standards and duties by failing to exercise reasonable care in  
 17 safeguarding and protecting Plaintiff's and Class members' PII and PHI by failing to design, adopt,  
 18 implement, control, direct, oversee, manage, monitor, and audit appropriate data security  
 19 processes, controls, policies, procedures, protocols, and software and hardware systems to  
 20 safeguard and protect PII and PHI entrusted to them - including Plaintiff's and Class members' PII  
 21 and PHI. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care  
 22 in safeguarding and protecting Plaintiff's and Class members' PII and PHI by failing to design,  
 23 adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security  
 24 processes, controls, policies, procedures, protocols, and software and hardware systems would  
 25 result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members'  
 26 PII and PHI.

27                     93. Defendants, by and through their negligent actions, inaction, omissions, and want of  
 28 ordinary care, unlawfully breached their duties to Plaintiff and Class members by, among other

1 things, failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class  
2 members' PII and PHI within their possession, custody and control.

3 94. Defendants, by and through their negligent actions, inactions, omissions, and want of  
4 ordinary care, further breached their duties to Plaintiff and Class members by failing to design,  
5 adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls,  
6 policies, procedures, protocols, and software and hardware systems for complying with the  
7 applicable laws and safeguarding and protecting their PII and PHI.

8 95. But for Defendant's negligent breach of the above-described duties owed to Plaintiff  
9 and Class members, their PII and PHI would not have been released, disclosed, and/or  
10 disseminated without their authorization.

11 96. Plaintiff's and Class members' PII and PHI was transferred, sold, opened, viewed,  
12 mined and otherwise released, disclosed, and/or disseminated to unauthorized persons without  
13 their authorization as the direct and proximate result of Defendants' failure to design, adopt,  
14 implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies,  
15 procedures and protocols for complying with the applicable laws and safeguarding and protecting  
16 Plaintiff's and Class members' PII and PHI.

17 97. Defendants' above-described wrongful actions, inaction, omissions, and want of  
18 ordinary care that directly and proximately caused this ransomware attack constitute negligence.

19 98. As a direct and proximate result of Defendants' above-described wrongful actions,  
20 inaction, omissions, and want of ordinary care that directly and proximately caused the  
21 ransomware attack, Plaintiff and Class members have suffered (and will continue to suffer)  
22 ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in  
23 monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in  
24 monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the  
25 illegal sale of the compromised data on the dark web; expenses and/or time spent on credit  
26 monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card  
27 statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit  
28 scores and ratings; lost work time; and other economic and non-economic harm.



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**COUNT II**  
**NEGLIGENCE *PER SE***  
**(On Behalf of Plaintiff and the Nationwide Class)**

99. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

100. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendants had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' PHI.

101. Pursuant to HIPAA, Defendants had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

102. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

103. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendants had a duty to protect the security and confidentiality of Plaintiff's and Class Members' PII and PHI.

104. Defendants breached their duties to Plaintiff and Class Members under HIPAA, the Federal Trade Commission Act, and the Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

105. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

106. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

107. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or should have known that it was failing to meet its duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII and PHI.

1 108. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and  
2 Class members have suffered (and will continue to suffer) ongoing, imminent, and impending  
3 threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm;  
4 actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss  
5 of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on  
6 the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time  
7 spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time  
8 spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic  
9 and non-economic harm.

10 **COUNT III**  
11 **UNJUST ENRICHMENT**  
12 **(On Behalf of Plaintiff and the Nationwide Class)**

13 109. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set  
14 forth herein.

15 110. Plaintiff and Class members' PII and PHI has value that was conferred on  
16 Defendants. Moreover, Plaintiff and Class members conferred benefits on Defendants in the form  
17 of payments for medical and healthcare services, both directly and indirectly. Defendants had  
18 knowledge of the benefits conferred by Plaintiff and Class members and appreciated such benefits.  
19 Defendants should have used, in part, the monies Plaintiff and Class members paid to it, directly  
20 and indirectly, to pay the costs of reasonable data privacy and security practices and procedures.

21 111. Additionally, Defendants utilized Plaintiff and Class members' valuable PII and  
22 PHI for their own business purposes and because Plaintiff and Class members bestowed actual  
23 value on Defendants, Defendants were obligated to devote sufficient resources to implement  
24 reasonable data privacy and security practices and procedures.

25 112. Plaintiff and Class members have suffered actual damages and harm as a  
26 result of Defendants' conduct, inactions, and omissions. Defendants should be required to disgorge  
27 into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable  
28 proceeds received from Plaintiff and Class members, including damages equaling the difference  
in value between the medical and healthcare services that included the reasonable data privacy and

1 security practices and procedures Plaintiff and Class members paid for and the medical and  
2 healthcare services without the reasonable data privacy and security practices they actually  
3 received.

4 **COUNT IV**  
5 **VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW, CAL. BUS. & PROF.**  
6 **CODE §§ 17200, ET SEQ.**  
7 **(On Behalf of Plaintiff and the California Class)**

8 113. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully  
9 set forth herein.

10 114. Defendants have violated Cal. Business and Professions Code §17200 *et seq.* by  
11 engaging in unlawful and unfair practices as defined in Cal. Bus. Prof. Code §17200.

12 115. Defendants engaged in unfair acts and practices by failing to maintain reasonable  
13 security practices and procedures as alleged herein. These unfair acts and practices were immoral,  
14 unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and  
15 California Class Members. Defendants' practices were also contrary to legislatively declared and  
16 public policies that seek to protect consumer data and ensure that entities who are entrusted with  
17 personal data utilize appropriate security measures, as reflected by laws like the Federal Trade  
18 Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et seq.*), the Gramm-Leach-Bliley  
19 Act (15 U.S.C. § 6801), California's Confidentiality of Medical Information Act (Civil Code §56  
20 *et seq.*), California's unfair insurance practices statutes (Ins. Code §790 *et seq.*), California's  
21 Insurance Information and Privacy Protection Act (Ins. Code §791 *et seq.*), and California's data  
22 breach statute, Cal. Civ. Code § 1798.81.5. The harm these practices caused to Plaintiff and the  
23 California Class Members outweighed their utility, if any.

24 116. Defendants engaged in unlawful business practices by violating the privacy and  
25 security requirements of HIPAA (42 U.S.C. § 1302d *et seq.*).

26 117. Defendants engaged in unlawful business practices by violating California's  
27 Confidentiality of Medical Information Act (Civil Code §56 *et seq.*) with respect to California  
28 Class members participating in health services plans regulated by the Knox-Keene Act.

1 118. Defendants engaged in unlawful business practices by violating Cal. Civ. Code §  
2 1798.82.

3 119. As a direct and proximate result of Defendants acts of unfair and unlawful practices  
4 and acts, the Plaintiff was injured and lost money or property, including but not limited to the loss  
5 of her legally protected interest in the confidentiality and privacy of her PII and PHI, and additional  
6 losses described above.

7 120. Defendants knew or should have known that their computer systems and data  
8 security practices were inadequate to safeguard California Class Members' PII and PHI and that  
9 the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the unfair  
10 practices and unlawful acts alleged herein were negligent, knowing and willful, and/or wanton and  
11 reckless with respect to the rights of members of the California Class.

12 121. California Class Members seek relief under Cal. Bus. & Prof. Code § 17200, *et.*  
13 *seq.*, including, but not limited to, restitution to Plaintiff and Class Members of money or property  
14 that the Defendants may have acquired by means of Defendants' unlawful and unfair business  
15 practices, restitutionary disgorgement of all profits accruing to Defendants because of their  
16 unlawful and unfair business practices, declaratory relief, attorney's fees and costs (pursuant to  
17 Cal. Code Civil Pro. §1021.5), and injunctive or other equitable relief.

18 **COUNT V**  
19 **VIOLATION OF CALIFORNIA'S CONFIDENTIALITY OF MEDICAL INFORMATION**  
20 **ACT, CAL. CIV. CODE § 56 ET SEQ.**  
21 **(On Behalf of Plaintiff and the California Class)**

22 122. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully  
23 set forth herein.

24 123. Defendants are "Contractors" as defined by Cal. Civ. Code § 56.05(d) and/or  
25 "Providers of Health Care" as defined by § 56.06, and therefore are subject to the requirements of  
26 the CMIA, Cal. Civ. Code §§ 56.10(a), (d), and € 56.101(a) and (b), 56.26(a), and 56.36(b).

27 124. Plaintiff and Class members are "Patients" as defined by Cal. Civ. Code § 56.06(k).

28 125. The Plaintiff and Class members' information that was the subject of the Data  
Breach included "Medical Information" as defined by Cal. Civ. Code § 56.05(j).

1 126. In violation of Cal. Civ. Code § 56.10(a), Defendants disclosed medical information  
2 without first obtaining an authorization. The unauthorized disclosure of Plaintiff's and Class  
3 members' PII and PHI to unauthorized individuals resulted from the affirmative actions and  
4 omissions of Defendants. Plaintiffs' and Class Members' PII and PHI was viewed by unauthorized  
5 individuals as a direct and proximate cause of Defendants' violation of Cal. Civ. Code § 56.10(a).

6 127. In violation of Cal. Civ. Code § 56.101(a), Defendants created, maintained,  
7 preserved, stored, abandoned, destroyed, or disposed of medication information (including  
8 Plaintiff's and Class members PII and PHI) in a manner that failed to preserve and breached the  
9 confidentiality of the information contained therein. This violation resulted from the affirmative  
10 actions and omissions of Defendants. Plaintiff's and Class Members' PII and PHI was viewed by  
11 unauthorized individuals as a direct and proximate cause of Defendants' violation of Cal. Civ.  
12 Code § 56.101(a).

13 128. In violation of Cal. Civ. Code § 56.101(a), Defendants negligently created,  
14 maintained, preserved, stored, abandoned, destroyed, or disposed of medical information  
15 (including Plaintiff's and Class members PII and PHI). Plaintiffs' and Class Members' PII and PHI  
16 was viewed by unauthorized individuals as a direct and proximate cause of Defendants' violation  
17 of Cal. Civ. Code § 56.101(a).

18 129. Plaintiff and Class members' PII and PHI that was the subject of the Data Breach  
19 included "electronic medical records" or "electronic health records" as set forth in Cal. Civ. Code §  
20 56.101(c) and defined by 42 U.S.C. § 17921(5).

21 130. In violation of Cal. Civ. Code § 56.101(b)(1)(A), Defendants' electronic health  
22 record system or electronic medical record system failed to protect and preserve the integrity of  
23 electronic medical information (including Plaintiff's and Class members' PII and PHI). This  
24 violation resulted from the affirmative actions and omissions of Defendants. Plaintiff's and Class  
25 Members' PII and PHI was viewed by unauthorized individuals as a direct and proximate cause of  
26 Defendants' violation of Cal. Civ. Code § 56.101(b)(1)(A).

27 131. In violation of Cal. Civ. Code § 56.26(a), Defendants, entities engaged in the  
28 business of furnishing administrative services to programs that provide payment for health care

1 services, knowingly used, disclosed, or permitted the disclosure of medical information (including  
2 Plaintiff's and Class members' PII and PHI) possessed in connection with performing  
3 administrative functions for a program, or in a manner not reasonably necessary in connection with  
4 the administration or maintenance of the program, or in a manner not required by law, or without  
5 authorization. This violation resulted from the affirmative actions and omissions of Defendants.  
6 Plaintiff's and Class Members' PII and PHI was viewed by unauthorized individuals as a direct  
7 and proximate cause of Defendants' violation of Cal. Civ. Code § 56.26(a).

8 132. In violation of Cal. Civ. Code § 56.10(e), Defendants further disclosed Plaintiff's  
9 and Class members' PII and PHI to persons or entities not engaged in providing direct healthcare  
10 services to Plaintiff or Class members or their providers of health care or health care service plans  
11 or insurers or self-insured employers.

12 133. Plaintiff and Class members were injured and have suffered damages, as described  
13 above, from Defendants' illegal disclosure and negligent release of their PII and PHI in violation of  
14 Cal. Civ. Code §§ 56.10, 56.101, 56.26, and 56.36 and therefore seek relief pursuant to Cal. Civ.  
15 Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of \$1,000,  
16 punitive damages of \$3,000, injunctive relief, and attorneys' fees, expenses and costs.

17 134. As a direct and proximate result of Defendants' violation of Cal. Civ. Code § 56, *et*  
18 *seq.*, Plaintiff and Class members now face an increased risk of future harm.

19 135. As a direct and proximate result of Defendants' violation of Cal. Civ. Code § 56, *et*  
20 *seq.*, Plaintiff and Class members have suffered injury and are entitled to damages in an amount to  
21 be proven at trial.

22 136. Plaintiff and Class members suffered a privacy injury by having their sensitive  
23 medical information disclosed, irrespective of whether or not they subsequently suffered identity  
24 theft or incurred any mitigation damages. Medical information has been recognized as private  
25 sensitive information in common law and federal and state statutory schemes and the disclosure of  
26 such information resulted in cognizable injury to Plaintiff and Class members.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, individually and on behalf of the members of the Class defined above, respectfully request that this Court:

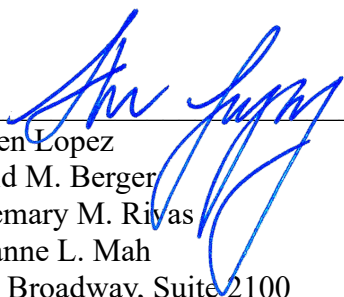
- (a) An order certifying this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;
- (b) A judgment awarding Plaintiff and Class members appropriate monetary relief, including actual damages, statutory damages, punitive damages, equitable relief, restitution, and disgorgement;
- (c) An order entering injunctive and declaratory relief as appropriate under the applicable law;
- (d) An order awarding Plaintiff and the Class pre-judgment and/or post-judgment interest as prescribed by law;
- (e) An order awarding reasonable attorneys' fees and costs as permitted by law; and
- (f) Any and all other and further relief as may be just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands a jury trial.

Dated: March 12, 2024

**GIBBS LAW GROUP LLP**



---

Steven Lopez  
David M. Berger  
Rosemary M. Rivas  
Rosanne L. Mah  
1111 Broadway, Suite 2100  
Oakland, California 94607  
(510) 350-9700 (tel.)  
(510) 350-9701 (fax)  
sal@classlawgroup.com  
rmr@classlawgroup.com  
dmb@classlawgroup.com  
rlm@classlawgroup.com

*Counsel for Plaintiff and the proposed Class*