

**WHATLEY KALLAS, LLP**

Alan M. Mansfield, SBN: 125998  
1 Sansome Street, 35th Floor  
PMB #131  
San Francisco, CA 94104  
Phone: (619) 308-5034  
Fax: (888) 341-5048  
Email: amansfield@whatleykallas.com

**JANSSEN MALLOY LLP**

Megan A. Yarnall, SBN: 275319  
730 Fifth Street  
Eureka, CA 95501  
Phone: (707) 445-2071 ext. 223  
Fax: (707) 445-8305  
Email: myarnall@janssenlaw.com

**Attorneys for Plaintiff**

[Additional Counsel on Signature Page]

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

JOHN DOE, on behalf of himself and all others  
similarly situated and for the benefit of the general  
public,

Plaintiff,

v.

PARTNERSHIP HEALTHPLAN OF  
CALIFORNIA, and DOES 1 through 10, inclusive,

Defendants.

Case No.

**CLASS ACTION COMPLAINT FOR  
VIOLATIONS OF:**

- (1) Information Practices Act of 1977
- (2) Confidentiality of Medical Information Act
- (3) Invasion of Privacy
- (4) Unlawful and Unfair Business Practices
- (5) Declaratory Relief

**Jury Trial Demanded on All Causes of  
Action So Triable**

1 Plaintiff John Doe (“Plaintiff”),<sup>1</sup> brings this action on behalf of himself and all others similarly  
2 situated and for the benefit of the general public against Defendant Partnership HealthPlan of California  
3 (“PHC”) and DOES 1–10, inclusive (collectively referred to herein as “Defendants”). Plaintiff, through  
4 his undersigned counsel, alleges the following based on personal knowledge as to allegations regarding  
5 Plaintiff, and on information and belief as to all other allegations, which allegations are likely to have  
6 evidentiary support after a reasonable opportunity for investigation and discovery.

### 7 **SUMMARY OF THE ACTION**

8 1. This action arises from the failure by PHC to adequately secure the private, personal or  
9 medical information of Plaintiff and all others similarly situated who are all non-California citizens and  
10 residents who are present or former enrollees or employees of PHC or its health care service plans, and  
11 whose information was accessed and released or disclosed as a result of the Hive ransomware attack in  
12 or about March, 2022 and were sent notice of this attack in May 2022. As detailed more fully below, in  
13 March 2022 PHC was subject to a ransomware attack and accompanying data breach and theft by the  
14 Hive ransomware group (“Hive”). When compared to the data reported by HHS Office of Civil Rights  
15 for the last 24 months, this would be the 2<sup>nd</sup> largest health plan data breach in the United States. The Hive  
16 group reported that, on or about March 19, 2022, it had gained access to Defendant PHC’s computer  
17 network, deployed malware that encrypted data in PHC’s servers, and had acquired copies of 850,000  
18 personal unique records related to PHC enrollees, and over 400 gigabytes of enrollees’ personal  
19 information stored on Defendant PHC’s computer network servers. PHC has reported that, “[i]n the initial  
20 period after the March 19 system disruption, PHC operations were at a standstill.” PHC failed to take  
21 steps necessary to prevent such an attack and has refused to date to fully and adequately notify victims  
22 of this ransomware attack that their personal information was improperly accessed and stolen.

23 2. Defendants’ employees negligently created, maintained, preserved, and stored Plaintiff’s  
24 and Class members’ personally individually identifiable “medical information,” within the meaning of  
25 Civil Code section 56.05(i). Defendants’ actions resulted in this medical information being improperly  
26 accessed and copied by unauthorized third parties.

27 \_\_\_\_\_  
28 <sup>1</sup> Due to the sensitive nature of this action, Plaintiff has chosen to file under a pseudonym. (*See, e.g., Doe v. Kaweah Delta Hosp.*, 2010 U.S. Dist. LEXIS 135808 (E.D. Cal., Dec. 22, 2010); *Does I thru XXIII v. Advanced Textile Corp.* 214 F.3d 1058, 1067 (9th Cir. 2000).)

1           3.       In California, the protection of personal privacy is of paramount importance. Article 1,  
2 section 1 of the California Constitution guarantees consumers their right to privacy. In addition, as  
3 recognized by the California Legislature, the use of sophisticated computer information technology has  
4 greatly magnified the potential risk to individual privacy that occurs from the maintenance of personal  
5 information by entities such as Defendants, necessitating that the maintenance of personal information is  
6 subject to strict limits governed by numerous California statutes.<sup>2</sup>

7           4.       Medical information in California is considered to be among the most sensitive private  
8 personal information available.<sup>3</sup> “Medical Information” is defined by California’s Confidential Medical  
9 Information Act, Cal. Civ. Code sections 56, *et seq.* (“CMIA”) as:

10           any individually identifiable information, in electronic or physical form, in possession of or  
11 derived from a provider of health care, health care service plan, pharmaceutical company,  
12 or contractor regarding a patient’s medical history, mental or physical condition, or  
13 treatment.

14           “Individually identifiable” means that the Medical Information includes or contains any  
15 element of personal identifying information sufficient to allow identification of the  
16 individual, such as the patient’s name, address, electronic mail address, telephone number,  
17 or Social Security Number, or other information that, alone or in combination with other  
18 publicly available information, reveals the identity of the individual.<sup>4</sup>

19           5.       “Medical Information”, for purposes of this Complaint, thus refers to the above definition,  
20 and encompasses both Personal Health Information (“PHI”), and Personally Identifiable Information  
21 (“PII”), including Social Security numbers associated with individual health records within PHC’s  
22 computer systems.

23           6.       Since Medical Information encompasses such personal and revealing information, it is  
24 highly valued as a gateway to medical identity theft<sup>5</sup> and more general identity theft.<sup>6</sup> Medical  
25 Information has been found to command up to \$1,000 per individual record on the dark web.<sup>7</sup> Thus,  
26 organizations such as Defendants who are entrusted with this most sensitive and valuable data have a  
27 non-delegable duty to take particularly special care to maintain up-to-date information security practices

28 \_\_\_\_\_  
<sup>2</sup> See Cal. Civil Code § 1798.1(b) & (c).

<sup>3</sup> See, e.g., Cal. Civ. Code § 1798.140(ae)(2)(B) (as amended by Proposition 24) (defining health information as sensitive data).

<sup>4</sup> Cal. Civ. Code § 56.05(i).

<sup>5</sup> R. Kam, *et al*, *Medical Identity Theft: A Deadly Side Effect of Healthcare Data Breaches*, ID Experts (2017).

<sup>6</sup> Identity Theft Resource Center, *Data Breaches in the Healthcare Industry Continue Due to Availability of Valuable Information* (8/11/2020).

<sup>7</sup> M. Yao, *Your Electronic Medical Records Could be Worth \$1,000 to Hackers*, Forbes (4/18/17).

1 and keep apprised of industry-related threats as they arise. The threat from the Hive group of a  
2 ransomware attack was reasonably foreseeable to Defendants, as health care companies had been warned  
3 for almost a year of the potential for such an attack on their computer systems.

4 7. Public health agencies and service providers such as PHC are legally required and have a  
5 duty to keep their clients' personal and Medical Information private and secured. Defendants breached  
6 duties owed to Plaintiff and Class members by, *inter alia*, (i) not exercising reasonable care in retaining,  
7 maintaining, securing, and safeguarding current and former clients' nonpublic personal and Medical  
8 Information from being accessed and stolen by unauthorized persons; (ii) failing to implement processes  
9 to detect a breach or unauthorized access in a timely manner and to act upon any warnings or alerts that  
10 Defendants' security systems had been breached or improperly accessed; (iii) failing to timely disclose  
11 the facts surrounding this breach to Plaintiff and Class members; and (iv) failing to disclose that  
12 Defendants could not or did not adequately secure Plaintiff's or Class members' personal and Medical  
13 Information.

14 8. Under the CMIA and other provisions of state and federal law referenced herein, Plaintiff  
15 and all other persons similarly situated have a recognized right to confidentiality in their personal Medical  
16 Information and can reasonably expect that their Medical Information would be protected by Defendants  
17 from unauthorized access. When Plaintiff and all other persons similarly situated provided their Medical  
18 Information to PHC for the purpose of enrollment, maintaining an account with PHC, seeking coverage  
19 for medical treatment and/or otherwise availing themselves of health care services through PHC, they  
20 did so with the reasonable understanding and assurance that their most sensitive medical and personal  
21 information would be kept confidential and secure.

22 9. The Historical and Statutory Notes for the short title of the CMIA, section 56, support  
23 these reasonable expectations:

24 The Legislature hereby finds and declares that persons receiving health care services have  
25 a right to expect that the confidentiality of individual identifiable Medical Information  
26 derived by health service providers be reasonably preserved. It is the intention of the  
27 Legislature in enacting this act, to provide for the confidentiality of individually  
28 identifiable Medical Information, while permitting certain reasonable and limited uses of  
that information.

10. Consistent with that statutory purpose, the CMIA provides that "a provider of health care,  
health care service plan, or contractor shall not disclose Medical Information regarding a patient of the

1 provider of health care or an enrollee or subscriber of a health care service plan without first obtaining  
2 an authorization [ . . . ].” (Cal. Civ. Code § 56.10(a).) Defendants’ actions permitted the disclosure of the  
3 Medical Information at issue here to unauthorized third parties.

4 11. Additionally, Civ. Code Section 56.101(a) states, in relevant part, that every health care  
5 provider or health care service plan that creates, maintains, preserves, or stores Medical Information shall  
6 do so in a manner that preserves its confidentiality. Defendants’ actions establish that they did not  
7 maintain the Medical Information at issue in a manner that preserved its confidentiality, as it was able to  
8 be improperly accessed and copied by unauthorized third parties, including the Hive group. PHC’s failure  
9 to create, maintain, preserve, and store Medical Information in a manner that preserved the confidentiality  
10 of the information contained therein resulted in the illegal access, authorization, exfiltration, disclosure,  
11 negligent release and/or theft of 850,000 personal unique records and over 400 gigabytes of data related  
12 to PHC enrollees, which necessarily included PII, PHI and Medical Information.

13 12. Unfortunately for Plaintiff and other similarly situated individuals who either are or were  
14 enrolled with PHC, their personal information and sensitive Medical Information was not secured in the  
15 manner required under California law that would prevent such unauthorized access. What’s worse,  
16 despite Defendants’ obligations under the law to promptly notify affected individuals so they can take  
17 appropriate action, Defendants failed to promptly provide such notice in the most expedient time possible  
18 and without unreasonable delay, failed to include in the data breach notice a sufficient description of the  
19 data breach incident to comply with Civil Code Section 1798.29(d)(2)(E), and any other relevant laws,  
20 and failed to provide in the data breach notice the information needed by Plaintiff and other similarly  
21 situated individuals to enable them react appropriately to the breach, including taking whatever mitigation  
22 measures are necessary.

23 13. If a health care provider or health care service plan creates, maintains, preserves, or stores  
24 Medical Information in a negligent manner, it shall be subject to the remedies provided for under Civil  
25 Code Section 56.36, subdivision (b). As set forth herein, Defendants violated this provision.

26 14. The remedies provided for under Civil Code Section 56.36(b) allow private litigants to  
27 bring an action against an entity that has permitted the negligent release of confidential information or  
28 records or that failed to create, maintain, preserve, or store Medical Information in a manner that

1 preserves its confidentiality to seek injunctive relief and, among other remedies, statutory damages of  
2 one thousand dollars (\$1,000). In order to recover under this paragraph, it is not necessary that the  
3 plaintiffs suffered or were threatened with actual damages. (Cal. Civ. Code § 56.36(b)(1).) These  
4 remedies are in addition to any other remedies available at law. (Cal. Civ. Code § 56.36(b).) Plaintiff  
5 have submitted a demand for the payment of damages to Defendants. Plaintiff only seek injunctive and  
6 equitable relief at this time but reserve the right to seek damages if Defendants do not timely and fully  
7 respond to Plaintiff's claim.

8 15. PHC failed to implement and maintain reasonable security procedures and practices  
9 appropriate to the nature of the information at issue in order to protect Plaintiff's and others' personal  
10 information, which would include PHI, PII and Medical Information. PHC also disclosed and/or  
11 permitted the disclosure of their Medical Information to unauthorized persons.

12 16. Defendants disregarded the rights of Plaintiff and members of the Class by negligently  
13 failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and the Class  
14 members' personal and Medical Information was safeguarded, failing to take available steps to prevent  
15 an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols,  
16 policies and procedures regarding data access and encryption, even for internal use, as well as appropriate  
17 procedures that would prevent such intrusions through methods such as phishing, such as multi-factor  
18 authentication. As a result, the PHI, PII and Medical Information of hundreds of thousands of PHC  
19 enrollees was compromised through disclosure to unknown and unauthorized third parties. This data  
20 includes, but is potentially not limited to, enrollees' full names, Social Security numbers, dates of birth,  
21 Driver's License numbers, Tribal Identification numbers, medical record numbers, treat, diagnosis,  
22 prescription and other Medical Information, health insurance information, member portal username and  
23 password, email address, and street address.

24 17. Plaintiff and all other similarly situated enrollees in PHC's programs face a long-term  
25 battle against identity theft if their full names, Social Security numbers, Driver's License numbers, dates  
26 of birth, addresses, health information, and other contact information were contained in this unauthorized  
27 access and exfiltration. Plaintiff and the Class members have a continuing interest in ensuring that their  
28 information is and remains safe. As shown by PHC's total shutdown of its system for close to a month,

1 stolen Medical Information can be used to interrupt important medical services. This presents an  
2 imminent and impending continuing risk for Plaintiff and Class members, particularly where PHC refuses  
3 to disclose full and accurate details of the ransomware attack. Plaintiff and the Class are thus entitled to  
4 injunctive and other equitable relief. PHC's failure to adequately protect the nonpublic personal and  
5 Medical Information in their possession has likely caused, and will continue to cause, substantial harm  
6 and injuries to Plaintiff and Class members.

7 18. Plaintiff brings this action on behalf of himself and others similarly situated for injunctive  
8 and equitable relief that may be appropriate for the benefit of such persons and the general public,  
9 including costs and expenses of litigation, including attorneys' fees.

10 **JURISDICTION AND VENUE**

11 19. This Court has original jurisdiction over this action under 28 U.S.C. § 1332(d) because  
12 the amount in controversy exceeds the sum of \$5,000,000, exclusive of interest and costs, and is a class  
13 action in which at least one member of the Class (as defined below) is a citizen of a State different from  
14 Defendants.

15 20. Venue is appropriate in this District under 28 U.S.C. § 1391 because a substantial part of  
16 the events or omissions giving rise to the claim occurred in this District.

17 **PARTIES**

18 21. On personal knowledge, Plaintiff John Doe was a resident of Humboldt County in the  
19 State of California, and now resides in and is a citizen of Nevada. Plaintiff was an enrollee in and/or  
20 received benefits from PHC in that County and in this District. Plaintiff used medical services in that  
21 County and in this District, which were paid for and/or managed in whole or in part by PHC. Plaintiff,  
22 like each member of the Class, provided Defendants with individually identifiable information and  
23 confidential medical information, as it is defined by Civil Code section 56.05(i), in order to receive health  
24 care from Defendants.

25 22. On personal knowledge, Plaintiff John Doe's medical history, mental or physical  
26 condition, or treatment, including diagnosis and treatment dates, was created, maintained, preserved, and  
27 stored onto Defendants' computer network. Thus, many of his medical records were located in this  
28 District. Such medical information included or contained an element of personal identifying information  
sufficient to allow identification of the individual, such as Plaintiff's name, date of birth, address, and

1 Social Security number, and additionally likely medical record number, insurance provider, electronic  
2 mail address, telephone number, or other information that, alone or in combination with other publicly  
3 available information, reveals Plaintiff's identity.

4 23. On personal knowledge, Plaintiff John Doe has been injured in fact and lost money or  
5 property as a result of Defendants' misconduct in having his Medical Information likely disclosed to and  
6 stolen by third parties without his authorization, and the confidentiality and integrity of his Medical  
7 Information has been breached, lost, not preserved, and not protected. Since this breach took place,  
8 Plaintiff is concerned that confidential information about him has been compromised because he has had  
9 fraudulent charges appearing on his credit card post this breach. Plaintiff understands the importance of  
10 protecting the confidentiality of Medical Information. The protection of such information from  
11 unauthorized disclosure is thus important and material to him. In addition to the concerns expressed  
12 above, Plaintiff has experienced fear, anxiety, and worry caused by the unauthorized disclosure of his  
13 Medical Information by PHC since he became aware of it, and remains concerned about the status of this  
14 information.

15 24. Defendant PHC identifies itself as a government agency subject to the California  
16 Information Practices Act of 1977 that, among other things, manages Med-Cal beneficiaries who reside  
17 in various Northern California counties. PHC operates a managed health care system designed provide  
18 health care delivery to individuals in this District, including in Del Norte, Humboldt, Lake, Lassen,  
19 Marin, Mendocino, Modoc, Napa, Trinity, Shasta, Siskiyou, Solano, Sonoma, and Yolo Counties in  
20 Northern California. PHC only provides such services to individuals who reside in California pursuant  
21 to several State health programs. PHC is organized as a health insuring organization under California  
22 law. Defendant maintains regional offices in this District. PHC claims to currently serve approximately  
23 600,000 members. PHC is considered a "covered entity" for purposes of HIPAA.

24 25. The true names, roles, and capacities in terms of their involvement in the wrongdoing at  
25 issue, whether individual, corporate, associate, or otherwise, of Defendants named as DOES 1 through  
26 10, inclusive, are currently unknown to Plaintiff and, therefore, are named as Defendants under fictitious  
27 names. Plaintiff will identify these Defendants' true identities and their involvement in the wrongdoing  
28 at issue if and when they become known.

26. Defendants' conduct described herein including reviewing, approving, or ratifying the



1 conduct at issue was undertaken either directly by PHC or as an agent, servant, contractor, or employee  
 2 of PHC pursuant to California Civil Code Section 1798.19, and/or was performed within the course and  
 3 scope of their authority, agency, or employment. Defendants are thus jointly and severally responsible,  
 4 in whole or in part, for the conduct, damages, and injuries alleged herein.

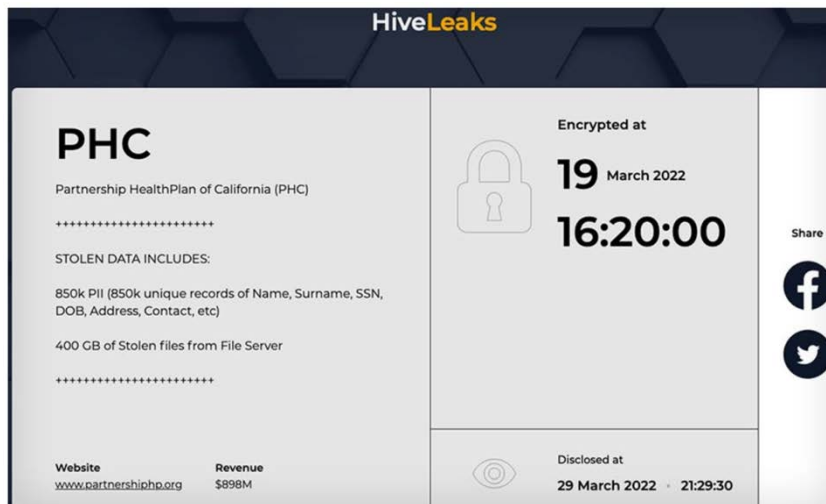
5 **FACTUAL ALLEGATIONS**

6 **A. THE NATURE OF THE RANSOMWARE ATTACK.**

7 27. On or about March 29, 2022, it was publicly reported that, in a ransomware event  
 8 occurring on March 19, 2022, PHC had 850,000 personal unique records exfiltrated by the Hive  
 9 ransomware group as part of a ransomware attack, including “Name, Surname, SSN, DOB, Address,  
 10 Contact, etc.” This group also reported it had stolen 400 Gigabytes of data from PHC file servers. It is  
 11 not clear when or how PHC eventually discovered this unauthorized access had taken place but if their  
 12 systems had been up to date they would have promptly discovered and/or prevented this improper access/.  
 13 If the Hive report is accurate, Defendants would have or should have discovered this breach when the  
 14 PHC data was encrypted by Hive on March 19.

15 28. The Hive ransomware group accessed and exfiltrated this data with the intent to misuse  
 16 it, including to demand ransom, marketing and/or selling this information on the dark web.

17 29. On or about March 29, 2022, the Hive Group published a website page entitled  
 18 “HiveLeaks” confirming that it had stolen Medical Information from PHC and then encrypted this  
 19 Medical Information on PHC servers on March 19, 2022. As reported by numerous public media sources,  
 20 the screenshot of HiveLeaks page regarding its theft of PHC data is shown here:



1           30.     On or about March 30, 2022, PHC shut down their entire patient-interfacing website.  
2 Critically, it did not tell and still has not told its members it had been subject to a ransomware attack, that  
3 over 850,000 unique records had been accessed and 400 Gigabytes of information had been stolen from  
4 PHC's file servers so that consumers could protect themselves. Rather, PHC uploaded the following  
5 message that cryptically read, in relevant part:

6           Partnership HealthPlan of California recently became aware of anomalous activity on  
7 certain computer systems within its network. We are working diligently with third-party  
8 forensic specialists to investigate this disruption, safely restore full functionality to affected  
9 systems, and determine whether any information may have been potentially accessible as  
10 a result of the situation.

11           31.     The only clue PHC provided that it had been subject to a ransomware attack and had  
12 Medical Information stolen from its servers was that it told patients on its replacement webpage that “[a]t  
13 this time, PHC is unable to receive or process Treatment Authorization Requests (TAR).” Treatment  
14 Authorization Requests are the forms required by PHC to gain pre-approved funding for treatment.  
15 Despite its duties and obligations under California law to promptly provide notice to consumers of such  
16 material facts so that they could take appropriate action, PHC did not inform members that it was  
17 experiencing a ransomware attack, that its systems had been encrypted by the Hive ransomware group,  
18 and that patient Medical Information had been stolen and disclosed.

19           32.     On or about April 15, 2022, PHC reported that it had restored its website functionality,  
20 only acknowledging there had been a “detection of anomalous activity within areas of the organization’s  
21 network.” However, PHC has not, as of that time, informed its members about that it was subject to a  
22 ransomware attack, nor offered them any compensation. As set forth below, the offer of a vague credit  
23 monitoring program is inadequate.

24           33.     On or about April 29, 2022, Plaintiff’s counsel sent a Notice of Violation to PHC and to  
25 the State of California, requesting, in part, that they provide immediate notice of this data breach to all  
26 similarly situated PHC members as to the scope and nature of this attack. The Notice notes that doing so  
27 is of particular immediate concern, as Plaintiff and others do not know what steps to take to protect their  
28 PII, and in many instances may not know that a data breach has even taken place. The notice provided  
by PHC in the last week does not comply with these requirements. Plaintiff does not assert claims for  
damages at this time but reserves the right to do so if Defendants do not timely respond to and accept

1 Plaintiff's claim for damages, on behalf of himself and all others similarly situated.

2 34. Starting on or about May 18, 2022, PHC began to notify state and federal officials and  
3 send out notices to present and former PHC enrollees regarding this attack. However, there are  
4 significant deficiencies in that notice. For example, California Civil Code § 1798.29(d)(2)(E) requires  
5 the notice contain, at a minimum, a "general description of the breach incident, if that information is  
6 possible to determine at the time the notice is provided." In this case, PHC has simply vaguely stated in  
7 its notice that it "identified unusual activity on its network," and that it has "evidence that an unauthorized  
8 party accessed or took certain information from PHC's network on or about March 19, 2022." This is not  
9 much different than its initial vague statement referenced above, where it stated on its website that PHC  
10 had become aware of "anomalous activity on certain computer systems within its network."

11 35. This brief and vague description is insufficient. As detailed above, PHC did not just suffer  
12 from "unusual activity" on certain computer servers – its entire system was subject to a ransomware  
13 attack, almost every enrollee in PHC was impacted by this attack as well as thousands of former enrollees,  
14 this attack was so significant that major aspects of PHC's computer systems were shut down for over a  
15 week as a result of the attack and impacted critical items such as scheduling of medical visits, and it  
16 appears that the stolen data is now available on the dark web. PHC was aware that Plaintiff's personal  
17 and Medical Information was stolen by the Hive ransomware group as part of that attack. By March 29,  
18 2022, the Hive group had taken credit for the theft and posted the categories of information stolen, along  
19 with the date and amount of data taken from PHC – **over 400 gigabytes of information**. By March 30,  
20 2022, media outlets had already begun to identify this "unusual activity" as a Hive ransomware attack.  
21 And, although it strains credibility to believe that PHC did not know they were subject to a ransomware  
22 attack by this point since its systems had been specifically encrypted by Hive on or about March 19,  
23 2022, on April 29, 2022, Plaintiff's Notice of Violation was sent by Plaintiff's counsel to PHC and  
24 identified the attack as a Hive ransomware event. None of this information was contained in the notice  
25 PHC sent to present and former enrollees.

26 36. Not only did PHC fail to provide a general description of the breach incident as required  
27 for purposes of statutory compliance, its vague and obfuscating language (for example, "accessed or took  
28 certain information," and "the information may include") unfairly prevents those individuals who have

1 been victimized in this attack from taking specific actions and mitigating measures that they might  
2 otherwise choose to if they were provided even the basic facts that this was a Hive ransomware attack  
3 and that that the group has taken credit for stealing 850,000 unique records of PII, including Name,  
4 Surname, Social Security number, Dates of Birth, Addresses and contact information.

5 37. These are significant discrepancies. For example, it would likely make a material  
6 difference to a consumer if his or her Medical Information and personal data was compromised by a  
7 group of teenagers, or researchers trying to alert PHC that its security systems are deficient, as opposed  
8 to that sensitive data was stolen by a gang of cyber-thieves and had been specifically identified as being  
9 located on the dark web. Knowledge that the latter has occurred highlights the need to take as many  
10 mitigation measures as possible and scrutinize future financial and medical statements for evidence of  
11 identity theft. PHC enrollees have not received disclosure of these material facts, which is material as  
12 numerous people have reported be subject to spam attacks and financial fraud since this breach took  
13 place.

14 **B. DEFENDANTS WERE ON NOTICE OF THE POTENTIAL FOR THIS ATTACK.**

15 38. PHC has been on notice for almost a year of the potential for a Hive ransomware attack  
16 on its systems but did not take sufficient steps to prevent it. Numerous news organizations reported on  
17 the threat specifically posed by the Hive group to health service providers following an attack attributed  
18 to them on Memorial Health Systems in August 2021.

19 39. Defendant PHC's negligence in safeguarding the Medical Information, PII and PHI of  
20 Plaintiff and the Class members was exacerbated by the repeated warnings and alerts directed to  
21 protecting and securing sensitive data, especially in light of the substantial increase in cyberattacks and/or  
22 data breaches in the healthcare and insurance industries preceding the date of this attack.

23 40. Specifically, as early as July 30, 2021, the U.S. Department of Health and Human Services  
24 ("HHS") issued an alert about the Hive group and its potential threat to healthcare organizations.<sup>8</sup>  
25 Referring to it as "nightmare," HHS recommended that healthcare organizations ensure they review the  
26 list of recommended mitigations in the Alert and promptly apply them to impacted systems in their

27 \_\_\_\_\_  
28 <sup>8</sup> See, HHS Cybersecurity Program H3: Section Alert (July 30, 2021), HiveNightmare/SeriousSAM  
Potential HPH Impact, [https://www.hhs.gov/sites/default/files/sector-alert-hive-nightmare-serious-sam-  
tlpwhite.pdf](https://www.hhs.gov/sites/default/files/sector-alert-hive-nightmare-serious-sam-<br/>tlpwhite.pdf) (last accessed 5/3/22).

1 infrastructure.<sup>9</sup>

2 41. On August 25, 2021, the HHS Cybersecurity Program published another Alert entitled  
 3 **Indicators of Compromise Associated with Hive Ransomware.**<sup>10</sup> The Alert was also widely circulated  
 4 and reported on by the media after its release.<sup>11</sup> HHS in particular noted that Hive had targeted entities  
 5 in the Healthcare and Public Health Sector. The Alert, issued in conjunction with the FBI, described how  
 6 the Hive group was operating, linked to an FBI Flash Alert that contained technical details about the Hive  
 7 ransomware group’s methods, sample ransom letters, and recommendations to detect, avoid and recover  
 8 from Hive’s intrusions.<sup>12</sup> The Alert contains a list of specific, technical indicators to immediately advise  
 9 companies such as PHC that a system has been compromised by the Hive ransomware group, recognizing  
 10 that awareness of these indicators could allow for detection during an attack and can help contain or  
 11 minimize its impact.<sup>13</sup>

12 42. According to the FBI Alert,

13 “Hive ransomware uses multiple mechanisms to compromise business networks, including  
 14 phishing emails with malicious attachments to gain access and Remote Desktop Protocol  
 (RDP) to move laterally once on the network.”

15 “After compromising a victim network, Hive ransomware actors exfiltrate data and encrypt  
 16 files on the network. The actors leave a ransom note in each affected directory within a  
 17 victim’s system, which provides instructions on how to purchase the decryption software.  
 The ransom note also threatens to leak exfiltrated victim data on the Tor site,  
 ‘HiveLeaks.’”<sup>14</sup>

18 43. In the FBI Flash Alert, the FBI specifically discourages the payment of ransom,  
 19 particularly as it may be a violation of federal law to do so.

20 “Paying a ransom may embolden adversaries to target additional organizations, encourage  
 21 other criminal actors to engage in the distribution of ransomware, and/or fund illicit

22 \_\_\_\_\_  
 23 <sup>9</sup> *Id.*

24 <sup>10</sup> HHS Cybersecurity Program HC3: Alert (August 25, 2021),  
<https://www.hhs.gov/sites/default/files/iocs-associated-with-hive-ransomware-alert.pdf> (last accessed  
 5/3/22).

25 <sup>11</sup> *See, e.g.*, FBI Flash TLP White: Indicators of Compromise Associated with Hive Ransomware –  
 August 25, 2021, American Hospital Association (8/25/21), <https://www.aha.org/fbi-tlp-alert/2021-08-25-fbi-flash-tlp-white-indicators-compromise-associated-hive-ransomware> (last accessed 5/3/22);

26 <sup>12</sup> *See*, FBI Flash TLP:White dated August 25, 2021,  
<https://www.ic3.gov/Media/News/2021/210825.pdf> (last accessed 5/3/21).

27 <sup>13</sup> HHS Cybersecurity Program HC3: Analyst Note (April 18, 2022),  
<https://www.hhs.gov/sites/default/files/hive-ransomware-analyst-note-tlpwhite.pdf> (last accessed  
 28 5/3/21).

<sup>14</sup> FBI Flash TLP White, n.12 *supra*, at 1.

1 activities. *Paying the ransom also does not guarantee that a victim's files will be recovered.*<sup>15</sup>

2 44. The FBI Flash Alert also contained recommended mitigations:

- 3
- 4 • Back-up critical data offline.
  - 5 • Ensure copies of critical data are in the cloud or on an external hard drive or storage device.
  - 6 • Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.
  - 7 • Use two-factor authentication with strong passwords, including for remote access services.
  - 8 • Monitor cyber threat reporting regarding the publication of compromised VPN login credentials and change passwords/settings if applicable. Keep computers, devices, and applications patched and up-to-date.
  - 9 • Install and regularly update anti-virus or anti-malware software on all hosts.<sup>16</sup>

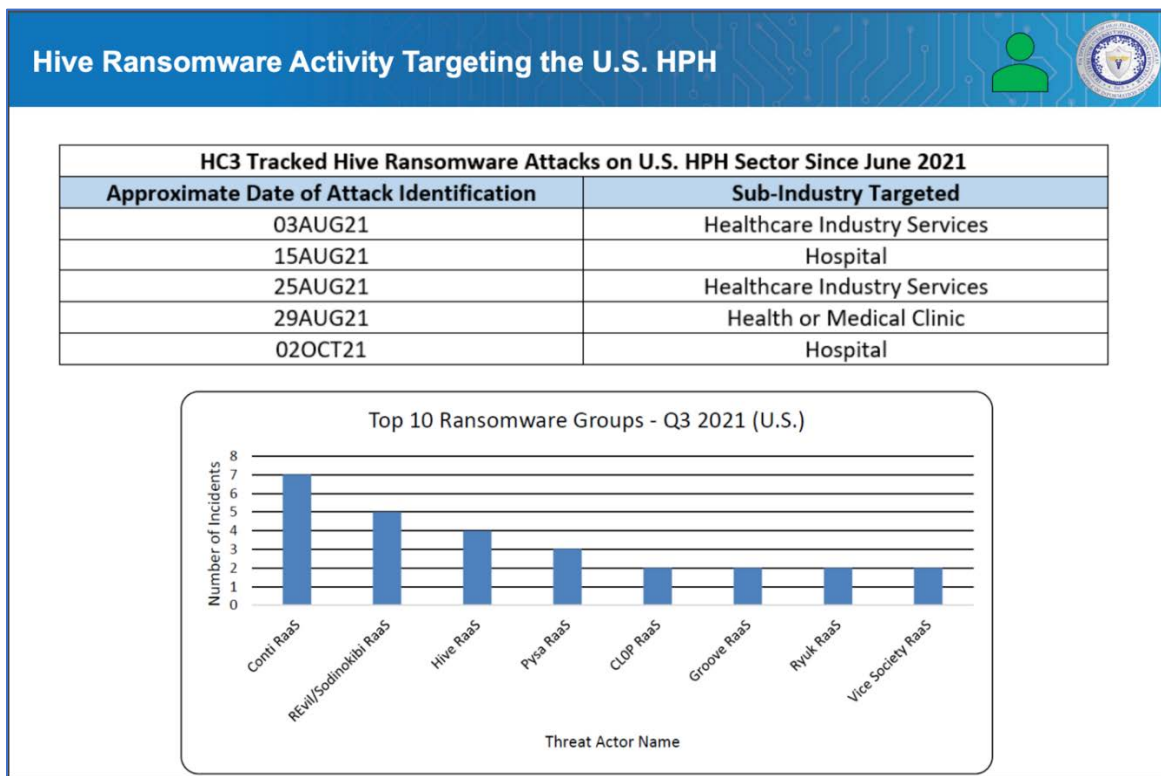
10 45. On October 21, 2021, HHS published yet another public document regarding Hive and  
11 the potential for a ransomware attack.<sup>17</sup> This document took the form of printed out PowerPoint slides  
12 that described the applications used by Hive, how the group gets initial access through phishing emails  
13 and remote desktop protocols, what Hive code looks like to detect it on company systems, and more.<sup>18</sup>  
14 HHS took pains to alert healthcare providers such as PHC that they were being targeted by Hive, as  
15 evidenced by the slide below:<sup>19</sup>

16  
17  
18  
19  
20  
21  
22  
23 \_\_\_\_\_  
24 <sup>15</sup> *Id.*, at 6 (emphasis added). This admonition comports with the trend noted by the Comparitech,  
25 which specializes in cyber security and privacy online, who also notes that "[t]here has also been a  
26 growing trend of double-extortion attempts in which hackers not only lock computers with a message  
27 demanding a ransom but also contact victims with proof of the data  
28 collected." <https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/>  
<sup>16</sup> *Id.* at 7-8. The August Alert also contains links to additional resources to prevent, protect and respond  
to ransomware events.

<sup>17</sup> *See*, HHS Cybersecurity Program Hive Ransomware (10/21/21), <https://www.hhs.gov/sites/default/files/hive-ransomware-1pwhite.pdf> (last accessed 5/3/22).

<sup>18</sup> *Id.*

<sup>19</sup> *Id.* at 8.



46. The October Alert also described how the attacks result in cancelled medical procedures and shut down patient care. Just as happened here, HHS noted that typically 62-400 gigabytes of information are stolen by the group, and the information exfiltrated contains Medical Information, financial information and other confidential data.<sup>20</sup>

### Hive Ransomware Activity Targeting the U.S. HPH (cont.)

Results of the attacks for patient services

- Canceled surgeries, diversion of ambulances, and closed urgent care units

Information Stolen

- 62–400 GB of information/data related to:
  - Medical records/care
  - Financial documents
  - Proprietary company work
  - Insurance forms, court documents
  - General work product, passwords
  - Employees' PII
  - Confidential clients' names

<sup>20</sup> *Id.* at 9.

1 47. HHS has analyzed Hive’s operations to be “standard practice amongst ransomware  
2 operators.”<sup>21</sup> As the HHS Analyst points out:

3 When defending against Hive or any other ransomware variant, there are standard practices  
4 that should be followed. *Prevention is always the optimal approach.* This includes but is  
not limited to the following:

- 5 • Use two-factor authentication with strong passwords – this is especially applicable  
for remote access services such as RDP and VPNs.
- 6 • Sufficiently backing up data, especially the most critical, sensitive and  
7 operationally necessary data is very important. We recommend the 3-2-1 Rule for  
the most important data: Back this data up in three different locations, on at least  
8 two different forms of media, with one of them stored offline.
- 9 • Continuous monitoring is critical, and should be supported by a constant input of  
threat data (open source and possibly proprietary as well)
- 10 • An active vulnerability management program must be comprehensive in scope and  
timely in implementation of the latest software updates. It should apply to  
11 traditional information technology infrastructure as well as any medical devices or  
equipment that is network-connected.
- 12 • Endpoint security should be comprehensive in scope and updated with the latest  
signatures/updates aggressively.<sup>22</sup>

13 48. Yet despite numerous attempts on the part of the federal government to inform healthcare  
14 organizations, like PHC, of the threat posed by ransomware attacks in general and Hive in particular, and  
15 despite having almost a year from their attack to prepare and prevent such an attack, PHC was negligent  
16 and did not adequately prepare for this wholly foreseeable event, allowing extremely sensitive data to be  
17 accessed, viewed and stolen by the Hive group.

18 49. As a result, despite requests to Defendants to take appropriate action prior to the filing of  
19 this Complaint, to date this unauthorized access, disclosure, and exfiltration remains fully unremedied.  
20 Defendants have failed to provide full and complete notice to affected consumers in the most expedient  
21 time possible and without unreasonable delay, as required under California law.

22 50. Defendants either knew, or reasonably should have known, the importance of  
23 safeguarding the Medical Information entrusted to them and of the foreseeable consequences if their  
24 computer network was breached. Defendants failed, however, to take adequate measures to prevent the  
25 Hive ransomware attack. Defendants were on notice that they should have and could have prevented this  
26 attack by properly securing and encrypting the Medical Information, PII and PHI of Plaintiff and the  
27

28 <sup>21</sup> HHS Cybersecurity Program HC3: Analyst Note, *supra*.

<sup>22</sup> *Id.* (*emphasis added*).



1 Class members and taking the steps outlined above to prevent infiltration by methods such as phishing  
2 by, for example using multi-factor authentication methods. Defendants could also have destroyed data of  
3 former enrollees that was no longer useful, especially outdated data.

4 51. The American Medical Association (“AMA”) has previously warned healthcare  
5 companies about the importance of protecting their patients’ confidential information:

6 Cybersecurity is not just a technical issue; it’s a patient safety issue. AMA research has  
7 revealed that 83% of physicians work in a practice that has experienced some kind of  
8 cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the  
9 privacy and security of patients’ health and financial information, but also patient access  
10 to care.<sup>23</sup>

11 52. Indeed, similar cyberattacks have become so notorious that the FBI and U.S. Secret  
12 Service back in 2019 issued a warning to potential targets such as PHC so they are aware of, and prepared  
13 for, a potential attack. As one report explained in an ominous foreshadowing of the events here,  
14 “[e]ntities like smaller municipalities and hospitals are attractive ... because they often have lesser IT  
15 defenses and a high incentive to regain access to their data quickly.” And according to the cybersecurity  
16 firm Mimecast, 90% of healthcare organizations had experienced cyberattacks just in the year prior to  
17 the issuance of that report.<sup>24</sup>

18 53. The healthcare industry in particular has experienced a large number of high-profile  
19 cyberattacks, placing Defendants on notice of the need to ensure their systems were not vulnerable to  
20 attacks such as they suffered here. Cybersecurity breaches hit an all-time high in 2021, exposing a record  
21 amount of patient PHI. In 2021, 45 million individuals were affected by healthcare attacks, up from 34  
22 million people in 2020.<sup>25</sup> Similarly, attacks against health plans jumped almost 35% from 2020 to 2021.<sup>26</sup>

23 54. For example, Universal Health Services experienced a cyberattack on September 29,  
24 2020, that appears similar to the ransomware attack on Defendants. As a result of this attack, Universal  
25 Health Services suffered a four-week outage of its systems, which caused as much as \$67 million in

26 <sup>23</sup> American Medical Assn (2018) Patient Safety: The Importance of Cybersecurity in Healthcare,  
27 <https://www.ama-assn.org/system/files/2018-10/cybersecurity-health-care-infographic.pdf> (last accessed  
28 5/3/22).

<sup>24</sup> See, FBI, Secret Service Warn of Targeted Ransomware, Law360 (Nov. 18, 2019),  
<https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last  
accessed 5/3/22)

<sup>25</sup> Critical Insight, *Health Breach Report July-Dec 2021* (2022), p. 3.

<sup>26</sup> *Id.* at 6.

1 recovery costs and lost revenue.<sup>27</sup> Similarly, on or about May 1, 2021, Scripps Healthcare in San Diego  
2 suffered a cyberattack, an event that effectively shut down critical health care services for a month and  
3 left numerous patients unable to speak to physicians or access vital medical and prescription records, just  
4 as happened here.<sup>28</sup> A couple of months later in July 2021, University of California San Diego Health  
5 suffered a similar attack.<sup>29</sup>

6 55. The increase in such attacks, and the attendant risk of future attacks, was widely known  
7 within Defendant PHC's industry. Due to the high-profile nature of these breaches and attacks,  
8 Defendants either were or should have been on heightened notice and aware of such attacks occurring in  
9 the healthcare industry and, therefore, should have been on notice of its duty to be proactive in guarding  
10 against being subject to such attacks and adequately performed their duty of preparing for and  
11 immediately identifying such an attack.

12 56. Yet, despite the prevalence of public announcements of these data breach and data security  
13 compromises, Defendants failed to take appropriate steps to protect Plaintiff's and Class members'  
14 Medical Information from being compromised and failed to timely, properly, and appropriately notify  
15 such persons that such an attack had taken place and the nature of the exfiltrated data.

16 **C. DEFENDANTS HAD AN OBLIGATION TO PROTECT PERSONAL AND**  
17 **MEDICAL INFORMATION UNDER STATE AND FEDERAL LAW AND THE**  
18 **APPLICABLE STANDARD OF CARE.**

19 57. Defendants are required by the Cal IPA, the CMIA and various other laws and regulations  
20 to protect Plaintiff's and Class members' Medical Information and to handle notification of any breach  
21 in accordance with applicable breach notification statutes. Defendants also needed to segment data by,  
22 among other things, creating firewalls and access controls so that if one area of Defendants' network is  
23 compromised, hackers cannot gain access to other portions of Defendants' systems. Failing to do so  
24 results in acts of negligence *per se* by Defendants. These duties are established in numerous California

25 <sup>27</sup> [https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-](https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and)  
26 [fourth-quarter-and](https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and) (last accessed 5/3/22).

27 <sup>28</sup> [https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-](https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/)  
28 [systems-hit-by-](https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/)  
29 [cyberattack-2/2619540/](https://www.nbcsandiego.com/news/local/scripps-health-employees-regaining-access-to-internal-systems-hit-by-cyberattack-2/2619540/) (last accessed 5/3/22).

30 <sup>29</sup> *Data Breach at UC San Diego Health: Some Employee Email Accounts Impacted* (July 27, 2021),  
31 [https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-](https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-accounts-impacted/2670302/)  
32 [accounts-impacted/2670302/](https://www.nbcsandiego.com/news/local/data-breach-at-uc-san-diego-health-some-employee-email-accounts-impacted/2670302/) (last accessed 5/3/22).

1 statutes, including California Civil Code Sections 56.101, 1798.21, and 1798.26.

2 58. In addition, as Defendants are entities covered by the Health Insurance Portability and  
3 Accountability Act (“HIPAA”) (45 C.F.R. § 160.102), they are required to comply with the HIPAA  
4 Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for  
5 Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the  
6 Protection of Electronic Protected Health Information”), 45 C.F.R. Part 160 and Part 164, Subparts A  
7 and C, which establish national security standards and duties for Defendants’ protection of Medical  
8 Information maintained by them in electronic form.

9 59. HIPAA requires Defendants to “comply with the applicable standards, implementation  
10 specifications, and requirements” of HIPAA “with respect to electronic protected health information.”  
11 45 C.F.R. § 164.302.

12 “Electronic protected health information” is defined as “individually identifiable health  
13 information ... that is (i) transmitted by electronic media; maintained in electronic media.”  
14 45 C.F.R. § 160.103.

15 60. HIPAA’s Security Rule requires Defendants to: (a) Ensure the confidentiality, integrity,  
16 and availability of all electronic protected health information the covered entity or business associate  
17 creates, receives, maintains, or transmits; (b) Protect against any reasonably anticipated threats or hazards  
18 to the security or integrity of such information; (c) Protect against any reasonably anticipated uses or  
19 disclosures of such information that are not permitted; and (d) Ensure compliance by their workforce.

20 61. HIPAA also requires Defendants to “review and modify the security measures  
21 implemented ... as needed to continue provision of reasonable and appropriate protection of electronic  
22 protected health information.” 45 C.F.R. § 164.306(c), and also to “[i]mplement technical policies and  
23 procedures for electronic information systems that maintain electronic protected health information to  
24 allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R.  
25 § 164.312(a)(1).

26 62. The ransomware attack on Defendants, particularly in light of the information received by  
27 them almost a year before the attack, establishes they did not comply with these Rules. This attack  
28 resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with  
safeguards mandated by HIPAA regulations, including, but not limited to, the following:

- 1 (a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendants  
2 create, receive, maintain, and transmit, in violation of 45 C.F.R. section  
3 164.306(a)(1);
- 4 (b) Failing to implement technical policies and procedures for electronic information  
5 systems that maintain electronic PHI to allow access only to those persons or  
6 software programs that have been granted access rights, in violation of 45 C.F.R.  
7 section 164.312(a)(1);
- 8 (c) Failing to implement policies and procedures to prevent, detect, contain, and  
9 correct security violations, in violation of 45 C.F.R. section 164.308(a)(1);
- 10 (d) Failing to identify and respond to suspected or known security incidents and  
11 mitigate, to the extent practicable, harmful effects of security incidents that are  
12 known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);
- 13 (e) Failing to protect against any reasonably-anticipated threats or hazards to the  
14 security or integrity of electronic PHI, in violation of 45 C.F.R. section  
15 164.306(a)(2);
- 16 (f) Failing to protect against any reasonably anticipated uses or disclosures of  
17 electronic PHI that are not permitted under the privacy rules regarding individually  
18 identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);
- 19 (g) Failing to ensure compliance with HIPAA security standard rules by its workforce,  
20 in violation of 45 C.F.R. section 164.306(a)(4);
- 21 (h) Impermissibly and improperly using and disclosing PHI that is and remains  
22 accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, *et*  
23 *seq.*;
- 24 (i) Failing to effectively train all members of its workforce (including independent  
25 contractors) on the policies and procedures with respect to PHI as necessary and  
26 appropriate for the members of its workforce to carry out their functions and to  
27 maintain security of PHI, in violation of 45 C.F.R. sections 164.530(b) and  
28 164.308(a)(5); and

- 1 (j) Failing to design, implement, and enforce policies and procedures establishing  
2 physical and administrative safeguards to reasonably safeguard PHI in compliance  
3 with 45 C.F.R. section 164.530(c).

4 63. Defendants also violated the duties applicable to them under the Federal Trade  
5 Commission Act (15 U.S.C. § 45 *et seq.*) from engaging in “unfair or deceptive acts or practices in or  
6 affecting commerce.” The FTC pursuant to that Act has concluded that a company’s failure to maintain  
7 reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair  
8 practice” in violation of the FTC Act.<sup>30</sup>

9 64. As established by these laws, Defendants owed a duty to Plaintiff and Class members to  
10 exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the  
11 Medical Information in their possession from being compromised, lost, stolen, accessed, and misused by  
12 unauthorized persons. Defendants also owed a duty to Plaintiff and Class members to provide reasonable  
13 security in compliance with industry standards and state and federal requirements, and to ensure that their  
14 computer systems, networks, and protocols adequately protected this Medical Information and were not  
15 exposed to infiltration. This also included a duty to Plaintiff and the Class members to design, maintain,  
16 and test their computer systems to ensure that the Medical Information in their possession was adequately  
17 secured and protected; to create and implement reasonable data security practices and procedures to  
18 protect the Medical Information in their possession and avoid access to their systems through processes  
19 such as phishing, including adequately training employees and others who accessed information within  
20 their systems on how to adequately protect Medical Information and avoid permitting such infiltration  
21 such as by use of multi-factor authentication; to implement processes that would detect a breach of their  
22 data security systems in a timely manner and to act upon data security warnings and alerts in a timely  
23 fashion; to disclose if their computer systems and data security practices were inadequate to safeguard  
24 individuals’ Medical Information from theft; and to disclose in a timely and accurate manner when data  
25 breaches or ransomware attacks occurred.

26 65. Defendants owed these duties to Plaintiff and Class members because they were  
27 foreseeable and probable victims of any inadequate data security practices. Defendants affirmatively

28 \_\_\_\_\_  
<sup>30</sup> See, e.g., *FTC v. Wyndham Worldwide Corp.*, (3d Cir. 2015) 799 F.3d 236.

1 chose to design their systems with inadequate user authentication, security protocols and privileges, and  
2 set up faulty patching and updating protocols. These affirmative decisions resulted in Hive being able to  
3 execute the ransomware attack and exfiltrate the data in question, to the injury and detriment of Plaintiff  
4 and Class members. By taking affirmative acts inconsistent with these obligations that left PHC's  
5 computer system vulnerable to a ransomware attack, Defendants disclosed and/or permitted the  
6 disclosure of Medical Information to unauthorized third parties. Through such actions or inactions, PHC  
7 failed to preserve the confidentiality of various pieces of personal and Medical Information they were  
8 duty-bound to protect.

9 66. As a direct and proximate result of Defendants' actions, inactions, omissions, breaches of  
10 duties and want of ordinary care that directly and proximately caused or resulted in the ransomware attack  
11 and the resulting data breach, Plaintiff and Class members have suffered and will continue to suffer  
12 damages and other injury and harm in the form of, *inter alia*, (a) as Plaintiff has already experienced,  
13 present, imminent, immediate and continuing increased risk of identity theft, identity fraud and medical  
14 fraud -- risks justifying expenditures for protective and remedial services for which they are entitled to  
15 compensation, (b) invasion of privacy, (c) breach of the confidentiality of their Medical Information, (d)  
16 deprivation of the value of their PHI, for which there is a well-established national and international  
17 market, as well as statutory damages to which they are entitled even without proof of access or actual  
18 damages; (e) the financial and temporal cost of monitoring their credit reports, (f) increased risk of future  
19 harm, and/or (g) have suffered fear, anxiety, and worry caused by the unauthorized release of their  
20 Medical Information, all resulting in a loss of money or property related to Defendants' misconduct.

21 **D. THE VALUE OF PII, PHI AND MEDICAL INFORMATION SHOWS THAT**  
22 **PLAINTIFF AND OTHERS LOST VALUABLE MONEY OR PROPERTY AS A**  
23 **RESULT OF THIS ATTACK.**

24 67. It is well known that Medical Information is a valuable commodity<sup>31</sup> and the frequent  
25 target of hackers, such that Plaintiff and Class members would lose money or property if their data was  
26 permitted to be improperly accessed or stolen.

27 <sup>31</sup> See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable  
28 Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at \*3-4  
(2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a  
level comparable to the value of traditional financial assets.") (citations omitted).

1 68. Defendants either were or should have been aware that the Medical Information, PII and  
2 PHI they collect is highly sensitive and of significant value to those who would use it for wrongful  
3 purposes. As the FTC has reported, identity thieves can use this information to commit an array of crimes  
4 including identify theft, medical and financial fraud.<sup>32</sup> Medical identity theft is one of the most common,  
5 most expensive, and most difficult-to-prevent forms of identity theft.

6 69. Indeed, a robust cyber black market exists in which criminals post stolen Medical  
7 Information, PII and PHI on multiple underground Internet websites, commonly referred to as the dark  
8 web, to create fake insurance claims, purchase and resell medical equipment, or access prescriptions for  
9 illegal use or resale. Criminals often trade stolen Medical Information, PII and PHI on the “cyber black  
10 market” for years following a breach. For example, it is believed that certain PHI/PII compromised in  
11 the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-  
12 19-related benefits.<sup>33</sup> According to a 2017 Javelin strategy and research presentation, fraudulent activities  
13 based on data stolen in data breaches that is between two and six years old had increased by nearly 400%  
14 over the previous 4 years.<sup>34</sup>

15 70. According to Experian, one of the three major credit bureaus, medical records can be  
16 worth up to \$1,000 per person on the dark web, depending upon completeness.<sup>35</sup> PII and PHI can be sold  
17 at a price ranging from approximately \$20 to \$300.<sup>36</sup>

18 71. Medical identify theft can also result in inaccuracies in medical records and costly false  
19 claims. It can also have life-threatening consequences since if a victim’s health information is mixed with  
20 other records, it can lead to misdiagnosis or mistreatment. “Medical identity theft is a growing and  
21 dangerous crime that leaves its victims with little to no recourse for recovery,” reported Pam Dixon,  
22 executive director of World Privacy Forum. “Victims often experience financial repercussions and worse

23 \_\_\_\_\_  
24 <sup>32</sup> Federal Trade Commission, What To Know About Identity Theft,  
<https://consumer.ftc.gov/articles/what-know-about-identity-theft> (last accessed 5/3/22).

25 <sup>33</sup> Janelle Stecklein, *Director: 64,000-plus fraudulent unemployment claims 'mitigated'*, The Duncan  
26 Banner (June 24, 2020), [https://www.duncanbanner.com/news/director-64-000-plus-fraudulent-unemployment-claims-mitigated/article\\_dc446671-73a6-5e8a-b732-bcedba72b458.html](https://www.duncanbanner.com/news/director-64-000-plus-fraudulent-unemployment-claims-mitigated/article_dc446671-73a6-5e8a-b732-bcedba72b458.html) (last accessed 5/3/22).

27 <sup>34</sup> See, Brian Stack, *Here’s How Much Your Personal Information is Selling for on the Dark Web*  
28 (2017) <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed 5/3/22).

<sup>35</sup> *Id.*

<sup>36</sup> <https://www.privacyaffairs.com/dark-web-price-index-2021/>

1 yet, they frequently discover erroneous information has been added to their personal medical files due to  
2 the thief's activities."<sup>37</sup>

3 72. The Ponemon Institute found that medical identity theft can cost victims an average of  
4 \$13,500 to resolve per incident, and that victims often have to pay off the imposter's medical bills to  
5 resolve the breach.<sup>38</sup>

6 73. In another study by the Ponemon Institute in 2015, 31% of medical identity theft victims  
7 lost their healthcare coverage as a result of the incident, while 29% had to pay to restore their health  
8 coverage, and over half were unable to resolve the identity theft at all.<sup>39</sup>

9 74. Defendants have only offered two years of a vague credit monitoring service. This is  
10 inadequate to protect consumers. Once PHI, PII and Medical Information is stolen, particularly such as  
11 membership identification numbers or Social Security numbers, fraudulent use of that information and  
12 damage to victims may continue for years, as the fraudulent use of such data resulting from the attack  
13 may not come to light for years. According to the U.S. Government Accountability Office ("GAO"),  
14 which conducted a study regarding data breaches: "[L]aw enforcement officials told us that in some  
15 cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further,  
16 once stolen data have been sold or posted on the Web, fraudulent use of that information may continue  
17 for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot  
18 necessarily rule out all future harm."<sup>40</sup> The ramifications of Defendants' failure to keep the Medical  
19 Information in question secure from attack and then not advise affected persons of all the relevant facts  
20 is thus not temporary but long lasting, as the fraudulent use of that information and damage to victims  
21 may continue for more than two years. That is one of the reasons providing prompt notice to consumers

22 \_\_\_\_\_  
23 <sup>37</sup> Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, (2/7/14),  
24 <https://khn.org/news/rise-of-identity-theft/> (last accessed 5/3/22); *See also, Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), <https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare> (last accessed 5/3/22).

25 <sup>38</sup> Brian O'Connor, Healthcare Data Breach: What to Know About Them and What to Do After One,  
26 Experian (June 14, 2018), <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/> (last accessed 5/3/22).

27 <sup>39</sup> Ponemon Institute, *Fifth Annual Study on Medical Identity Theft*, (February, 2015),  
[http://www.medidfraud.org/wp-content/uploads/2015/02/2014\\_Medical\\_ID\\_Theft\\_Study1.pdf](http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf) (last  
28 accessed 5/3/22).

<sup>40</sup> *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, <https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm> (last accessed 5/3/22).



1 as expeditiously as possible is necessary, so they can take actions to protect themselves. Yet Defendants  
2 are still refusing to even acknowledge that a ransomware event took place, let alone providing timely,  
3 proper, and appropriately comprehensive notice in the most expedient time possible and without  
4 unreasonable delay, as required under California law.

5 **CLASS ALLEGATIONS**

6 75. Plaintiff, on behalf of himself and all others similarly situated, bring this action pursuant  
7 to Fed. R. Civ Proc. Rule 23. This action satisfies the numerosity, commonality, typicality, adequacy,  
8 predominance, and superiority requirements for class certification.

9 76. The proposed class (“Class”) is defined as:

10 All non-California citizens and residents who are present or former enrollees or employees  
11 of PHC or its health care service plans, and whose information was accessed and released  
12 or disclosed as a result of the Hive ransomware attack in or about March, 2022 and were  
13 sent notice of this attack in May 2022.<sup>41</sup>

14 77. Plaintiff reserves the right to modify or amend the definition of the proposed Class before  
15 the Court determines whether class certification is appropriate.

16 78. The members of the Class are sufficiently numerous such that joinder of all Class members  
17 is impracticable. The proposed Class contains PHC members and employees who were among the  
18 854,913 individuals who had their personal or medical information improperly accessed or taken. While  
19 the exact number of persons is currently known to PHC, notices have recently been sent by PHC  
20 nationwide to thousands of persons such as Plaintiff who, while members or employees of PHC while in  
21 California, have since moved from California.

22 79. Common questions of law and fact exist as to all members of the Class and predominate  
23 over questions affecting only individual Class members. The factual bases underlying Defendants’  
24 misconduct is common to all Class members and represents a common thread of unlawful and negligent  
25 conduct, resulting in injury to all members of the Class. These common legal and factual questions  
26 include the following:

27 (a) Whether Defendants implemented and maintained reasonable security practices and  
28 procedures appropriate to protect Plaintiff’s and Class members’ Medical Information from unauthorized

<sup>41</sup> Two actions on behalf of all California citizens and residents were filed on May 5 and 24, 2022,  
respectively, in Humboldt County Superior Court. See CV-22-00606 and CV-22-00719.

1 access, destruction, use, theft, modification, or disclosure;

2 (b) Whether Defendants and their employees, agents, officers, and/or directors negligently  
3 and/or unlawfully disclosed or permitted the unauthorized disclosure of Plaintiff's and Class members'  
4 Medical Information to unauthorized persons;

5 (c) Whether Defendants negligently created, maintained, preserved, stored, abandoned,  
6 destroyed, or disposed of Plaintiff's and Class members' Medical Information, and failed to protect and  
7 preserve the integrity of the Medical Information found on PHC's electronic health record systems or  
8 electronic medical record systems;

9 (d) Whether Defendants' actions or inactions were a proximate result of the negligent release  
10 of confidential information or records concerning Plaintiff and the Class;

11 (e) Whether Defendants adequately, promptly, timely and accurately informed Plaintiff and  
12 the Class members that their Medical Information had been compromised and whether Defendants  
13 violated the law by failing to promptly notify Plaintiff and the Class members of this material fact;

14 (f) Whether Defendants have adequately addressed and fixed the vulnerabilities that  
15 permitted the ransomware attack and resulting data breach to occur;

16 (g) Whether Defendants engaged in "unfair" business practices by failing to safeguard the  
17 Medical Information of Plaintiff and the Class, and whether Defendants' violations of the state and  
18 federal laws cited herein constitute "unlawful" business practices in violation of California Business and  
19 Professions Code § 17200, et seq.;

20 (h) Whether Defendants violated California's Information Practices Act of 1977, the  
21 California Medical Information Act, and the other laws cited herein; and

22 (i) Whether Plaintiff and the Class are entitled to injunctive relief to redress the imminent  
23 and currently ongoing harm faced as a result of the ransomware attack and Defendants' failure to provide  
24 notice thereof, and the scope of such relief.

25 80. Plaintiff's claims are typical of the claims of other Class members. There is no unique  
26 defense available to Defendants as Plaintiff, like all Class members, was enrolled in PHC's health  
27 services plan and was apparently subjected to the unauthorized disclosure of Medical Information as a  
28 result of Defendants' conduct and unable to access certain aspects of Defendants' computer systems for

1 a month.

2 81. Plaintiff will fairly and adequately represent the interests of the Class members. Plaintiff  
3 have retained counsel with substantial experience in prosecuting complex litigation and class actions,  
4 including data breaches concerning the sensitive Medical Information of individuals. Plaintiff and his  
5 counsel are committed to vigorously prosecuting the action on behalf of the Class. Neither Plaintiff nor  
6 his counsel have any interest adverse to or that irreconcilably conflicts with those of other Class members.

7 82. Absent a class action, most members of the Class would find the cost of litigating their  
8 claims to be prohibitive and may have no effective and complete remedy and may not even learn of the  
9 wrongful conduct at issue. Class treatment of common questions of law and fact is also superior to  
10 multiple individual actions or piecemeal litigation and results in substantial benefits in that it conserves  
11 the resources of the courts and litigants and promotes consistency and efficiency of adjudication. The  
12 conduct of this action as a class action presents few management difficulties and protects the rights of  
13 each Class member. Plaintiff thus anticipates no difficulty in the management of this case as a class action  
14 and providing notice to members of the Class.

15 83. Class treatment is also appropriate because Defendants have acted on grounds generally  
16 applicable to members of the Class, making class-wide equitable, injunctive, declaratory, and monetary  
17 relief appropriate.

18 **CAUSES OF ACTION**

19 **FIRST CAUSE OF ACTION**

20 **Violation of the Information Practices Act of 1977**

21 **Cal. Civ. Code § 1798 *et seq.***

22 84. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein.

23 85. Cal. Civ. Code section 1798.21 requires agencies of the State of California to “establish  
24 appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with  
25 the provisions of this chapter [the Cal IPA], to ensure the security and confidentiality of records, and to  
26 protect against anticipated threats or hazards to their security or integrity which could result in any  
27 injury.” (bracketed text added for clarity) Defendant PHC has identified itself as an agency subject to the  
28 provisions of the Cal IPA.

1           86.     Cal. Civ. Code section 1798.3(g) defines the term “record” as “any file or grouping of  
2 information about an individual that is maintained by an agency by reference to an identifying particular  
3 such as the individual’s name, photograph, finger or voice print, or a number or symbol assigned to the  
4 individual.”

5           87.     Cal. Civ. Code section 1798.24 further requires that an agency shall not disclose any  
6 personal information in a manner that would link the information disclosed to the individual to whom it  
7 pertains unless the information is disclosed with the prior written voluntary consent of the individual to  
8 whom the information pertains, subject to certain caveats not relevant here.

9           88.     “Personal information” is defined to mean “any information that is maintained by an  
10 agency that identifies or describes an individual, including, but not limited to, his or her name, Social  
11 Security Number, physical description, home address, home telephone number, education, financial  
12 matters, and medical or employment history. It includes statements made by, or attributed to, the  
13 individual.” (Cal. Civ. Code § 1798.3(a)). For purposes of the Cal IPA’s data breach notification  
14 requirements, “personal information” has more limited meaning, but includes an individual’s first name  
15 or first initial and last name in combination with one or more of the following data elements: (a) Social  
16 Security number, (b) driver’s license number, (c) Medical Information, or (d) health insurance  
17 information.

18           89.     Cal. Civ. Code section 1798.29 requires that any agency that stores computerized data that  
19 includes personal information shall disclose any breach of the security of the system following discovery  
20 of notification of the breach in the security of the data to any resident of California, when such personal  
21 information is unencrypted and was, or is reasonably believed to have been, acquired by an unauthorized  
22 person. (Cal. Civ. Code § 1798.29(a)). Any agency likewise has a duty to inform California residents of  
23 a breach in the security of their data, if the personal information is encrypted, but the encryption key or  
24 security credential was, or is reasonably believed to have been, acquired by an unauthorized person and  
25 the agency has a reasonable belief that the encryption key or security credential could render that personal  
26 information readable or usable. (Cal. Civ. Code § 1798.29(b)).

27           90.     The notification required under California Civil Code section 1798.29 must be made in  
28 the most expedient time possible and without unreasonable delay.

1           91. A data breach notification under the Cal IPA must meet specific content and format  
2 requirements as set forth in Civil Code section 1798.29(d), designed to call attention to the nature and  
3 the significance of the information it contains and including, but not limited to the types of personal  
4 information reasonably believed to have been the subject of the breach, the date of the breach, a general  
5 description of the data breach incident, and the toll-free numbers and addresses of the major credit  
6 reporting agencies, if as here the breach exposed a Social Security Number or California identification  
7 card number.

8           92. PHC's actions and inactions constitute a violation of a mandatory duty. The injury to  
9 Plaintiff and the Class is the kind of injury that the Cal IPA was designed to protect against, and their  
10 injury was proximately caused by PHC's failure to discharge its mandatory duty. PHC has failed to  
11 exercise reasonable diligence to discharge that duty.

12           93. Defendants' conduct violates the Cal IPA in at least the following ways:

- 13           (a) Defendants requested and came into possession of Plaintiff's and Class members'  
14 personal and Medical Information as a state agency to accomplish the agency's  
15 function as a health care service plan and had a statutory duty to exercise  
16 reasonable care in preserving the security and confidentiality of this information.
- 17           (b) Plaintiff and Class members, as enrollees in PHC's programs, had their personal  
18 and Medical Information negligently stored within Defendants' databases.
- 19           (c) Defendants maintained Plaintiff's and Class members' personal information as  
20 defined by the Cal IPA and disclosed that personal information in a manner that  
21 would link the information to the Plaintiff or Class member to whom the  
22 information pertained to unauthorized actors, including but not limited to the Hive  
23 ransomware group, without Plaintiff's or Class members' voluntary written  
24 consent.
- 25           (d) Defendants were entrusted with Plaintiff's and Class members' personal and  
26 Medical Information, and therefore were required "to ensure the security and  
27 confidentiality of records, and to protect against anticipated threats or hazards to  
28 their security or integrity which could result in any injury."

1 (e) Defendants were required to “establish appropriate and reasonable administrative,  
2 technical, and physical safeguards to ensure compliance” with the Cal IPA, to  
3 ensure the security and confidentiality of records, and to protect against anticipated  
4 threats or hazards to their security or integrity which could result in any injury”.

5 (f) Defendants failed to ensure the security and confidentiality of Plaintiff’s and Class  
6 members’ records containing Medical Information.

7 (g) Defendants failed to protect Plaintiff’s and Class members’ records containing  
8 Medical Information against anticipated threats or hazards to their security or  
9 integrity, which could result in injury by failing to protect against the known Hive  
10 ransomware attack affecting those records in March 2022, as described above.  
11 This attack was a threat or hazard to the security and/or integrity of that  
12 information that should have been anticipated by Defendants as having the  
13 potential to cause injury.

14 (h) Defendants failed to “establish appropriate and reasonable administrative,  
15 technical, and physical safeguards to ensure compliance” with the Cal IPA, as  
16 evidenced by its failure to prevent or promptly identify the Hive ransomware  
17 attack affecting Plaintiff’s and Class members’ records in March 2022, as  
18 described above.

19 (i) Defendants have failed to timely and/or adequately notify affected California  
20 residents about the breach in the security of their personal data, as required under  
21 California Civil Code section 1798.29(a).

22 94. As a result of Defendants’ failure to comply with and/or ensure compliance with the Cal  
23 IPA, Plaintiff and members of the Class have suffered injury.

24 95. Unless and until enjoined and restrained by order of this Court, and compliance with the  
25 notice requirements be immediately undertaken, Defendants’ wrongful conduct will continue to cause  
26 Plaintiff and the Class injury.

27 96. Plaintiff seeks injunctive relief, fees and costs of suit as permitted by this statute. Plaintiff  
28 will amend this claim to seek damages if Defendants do not timely or adequately respond to the Notice

1 of Violation and claims submitted by Plaintiff’s counsel referenced above.

2 **SECOND CAUSE OF ACTION**

3 **Violation of the Confidentiality of Medical Information Act**

4 **Cal. Civ. Code § 56 *et seq.***

5 97. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein.

6 98. Defendant PHC is a “health care service plan” as defined by Cal. Civ. Code section  
7 56.05(f) and is therefore subject to the requirements of the CMIA.

8 99. As a health care service plan, PHC must not disclose or permit the disclosure of Medical  
9 Information regarding a patient of the provider of health care or an enrollee or subscriber of a health care  
10 service plan without first obtaining authorization, subject to certain exceptions found in Civil Code  
11 Section 56.10(b) & (c) that do not apply here. (Cal. Civ. Code § 56.10(a).) By their affirmative acts and  
12 inactions set forth above, Defendants disclosed or permitted the disclosure of Medical Information to  
13 unauthorized third parties, in violation of this Section.

14 100. As a health care service plan, Defendant is required under the CMIA to ensure that it  
15 maintains, preserves, and stores Medical Information in a manner that preserves the confidentiality of the  
16 information contained therein. (Cal. Civ. Code § 56.101(a) & 56.36(b).)

17 101. As a health care service plan, PHC is required to create, maintain, preserve, store,  
18 abandon, destroy or dispose of Medical Information in a non-negligent manner. (Cal. Civ. Code §  
19 56.101(a).)

20 102. Under the CMIA, electronic health record systems or electronic medical record systems  
21 are required to protect and preserve the integrity of electronic Medical Information. (Cal. Civ. Code §  
22 56.101(b)(1)(A).) The term “electronic health record” or “electronic medical record” means an electronic  
23 record of health-related information on an individual that is created, gathered, managed, and consulted  
24 by authorized health care clinicians and staff. (Cal. Civ. Code § 56.101(c) as defined by 42 U.S.C. §  
25 17921(5).)

26 103. Plaintiff and members of the Class are “Patients” as defined by Cal. Civ. Code section  
27 56.05(j).

28 104. The information at issue in this action is “Medical Information” as that term is defined by

1 section 56.05(i) of the CMIA.

2 105. As described above, the actions or inactions of PHC failed to preserve the confidentiality  
3 of Medical Information, including but not limited to: Plaintiff’s and Class members’ full names, dates of  
4 birth, addresses, Social Security numbers, as well as likely insurance provider information, and public  
5 health program participant information that, either alone or in combination with other publicly available  
6 information, reveals their identities.

7 106. The Medical Information that was the subject of the ransomware attack and resulting data  
8 breach detailed above was accessed, removed and viewed by the Hive ransomware group and its  
9 members, and other unauthorized parties during and following the ransomware attack.

10 107. Since the Hive ransomware group was able to identify the contents of the 400 gigabytes  
11 of information it stole from PHC, as well as publicly reporting that the data stolen from PHC also included  
12 850,000 PII such as “unique records of Name, Surname, SSN, DOB, Address, Contact, etc,” the Hive  
13 ransomware group necessarily viewed the data at issue herein and the confidentiality and integrity of that  
14 data was breached, lost, not preserved, and not protected by Defendants.

15 108. In violation of the CMIA, Defendants disclosed or permitted the disclosure of Medical  
16 Information regarding Plaintiff and Class members without authorization to a third party. This disclosure  
17 did not qualify for any of the exemptions set forth in Civil Code Section 56.10(b) or (c), which provide  
18 limited bases for allowing unauthorized disclosures. This disclosure of Medical Information to  
19 unauthorized individuals resulted from the affirmative actions and inactions of Defendants and their  
20 employees, which allowed hackers from the Hive ransomware group to access, view and obtain the  
21 Medical Information of hundreds of thousands of PHC members.

22 109. In violation of the CMIA, Defendants created, maintained, preserved, stored, abandoned,  
23 destroyed, or disposed of Medical Information of Plaintiff and Class members in a manner that did not  
24 preserve the confidentiality of the information contained therein.

25 110. In violation of the CMIA, Defendants negligently created, maintained, preserved, stored,  
26 abandoned, destroyed, or disposed of Medical Information of Plaintiff and Class members.

27 111. In violation of the CMIA, PHC’s electronic health record systems or electronic medical  
28 record systems did not protect and preserve the integrity of Plaintiff’s and Class members’ Medical



1 Information.

2 112. In violation of the CMIA, Defendants negligently released confidential information or  
3 records concerning Plaintiff and Class members.

4 113. In violation of the CMIA, Defendants failed to give prompt, timely and fulsome notice of  
5 the Hive ransomware attack and resulting data breach.

6 114. As a direct and proximate result of Defendants' wrongful actions, inactions, omissions,  
7 and want of ordinary care that directly and proximately caused the release of Medical Information of  
8 hundreds of thousands of individuals, such personal Medical Information was viewed by, released to,  
9 and disclosed to third parties without appropriate written authorization.

10 115. Plaintiff and Class members are therefore entitled to injunctive relief and reasonable  
11 attorneys' fees and costs.

12 116. If Defendants do not timely respond to Plaintiff's claims for payment of damages  
13 submitted by Plaintiff's counsel prior to the initiation of this action, Plaintiff will amend this Complaint  
14 to seek actual damages, statutory damages of \$1,000 per Class member and punitive damages of \$3,000  
15 per Class member.

16 **THIRD CAUSE OF ACTION**

17 **Invasion of Privacy**

18 **California Constitution, Article I, Section 1**

19 117. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein.

20 118. The California Constitution provides: "All people are by nature free and independent and  
21 have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possession,  
22 and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const., Art. I.,  
23 § 1.

24 119. Plaintiff and Class members had a legitimate expectation of privacy in their Medical  
25 Information, PII and PHI, and were entitled to the protection of this information against disclosure to  
26 unauthorized third parties.

27 120. Defendants owed a duty to Plaintiff and Class members to keep their Medical Information,  
28 PII and PHI confidential.

1 121. Defendants failed to protect and released to unauthorized third parties the non-redacted  
2 and non-encrypted Medical Information, PII and PHI of Plaintiff and Class members.

3 122. Defendants allowed unauthorized and unknown third parties access to and examination of  
4 the Medical Information, PII and PHI of Plaintiff and Class members by way of Defendants' affirmative  
5 actions and negligent failures to protect this information.

6 123. The unauthorized release to, custody of, and examination by unauthorized third parties of  
7 the Medical Information, PII and PHI of Plaintiff and Class members is highly offensive to a reasonable  
8 person.

9 124. The intrusion at issue was into a place or thing, which was private and is entitled to be  
10 private. Plaintiff and Class members disclosed their Medical Information, PII and PHI to Defendants as  
11 part of Plaintiff's and Class members' relationships with Defendants, but privately and with the intention  
12 that the Medical Information, PII and PHI would be kept confidential and would be protected from  
13 unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such  
14 information would be kept private and would not be disclosed without their authorization.

15 125. The Hive ransomware attack that resulted from the actions and inactions of Defendants  
16 constitutes an intentional interference with the Plaintiff's and Class members' interest in solitude or  
17 seclusion, either as to their persons or as to their private affairs or concerns and those of their families,  
18 of a kind that would be highly offensive to a reasonable person.

19 126. Defendants acted with a knowing or negligent state of mind when they permitted the attack  
20 described herein to occur, because they either knew or reasonably should have known that their  
21 information security practices were inadequate and insufficient to protect against such attacks.

22 127. Defendants either knew or reasonably should have known that their inadequate and  
23 insufficient information security practices would cause injury and harm to Plaintiff and Class members.

24 128. As a proximate result of the above acts and omissions of Defendants, the Medical  
25 Information, PII and PHI of Plaintiff and Class members was disclosed to third parties without  
26 authorization, causing Plaintiff and Class members to suffer injuries and damages. Plaintiff will amend  
27 this claim to seek damages in an amount according to proof at time of trial if Defendants do not timely  
28 or adequately respond to the Notice of Violation and claims submitted by Plaintiff's counsel referenced

1 above.

2 129. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful  
3 conduct will continue to cause irreparable injury to Plaintiff and the Class, entitling them to seek  
4 injunctive relief.

5 130. This action, if successful, will enforce an important right affecting the public interest and  
6 would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons and/or  
7 the general public. Private enforcement is necessary and places a disproportionate financial burden on  
8 Plaintiff in relation to Plaintiff's stake in the matter. Because this case is brought for the purposes of  
9 enforcing important rights affecting the public interest, Plaintiff also seeks the recovery of attorneys' fees  
10 and costs in prosecuting this action against Defendants under Code of Civil Procedure section 1021.5 and  
11 other applicable law.

#### 12 **FOURTH CAUSE OF ACTION**

#### 13 **Violation of the Unfair Competition Law**

#### 14 **Cal. Bus. & Prof. Code § 17200 *et seq.***

15 131. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein.

16 132. The acts, misrepresentations, omissions, practices, and non-disclosures of Defendants as  
17 alleged herein constituted unlawful and unfair business acts and practices within the meaning of  
18 California Business & Professions Code sections 17200, *et seq.*

19 133. Defendants engaged in "unlawful" business acts and practices in violation of the  
20 California statutes set forth above, including Civil Code sections 56.10(a), 56.101, 1798.21, 1798.29 and  
21 Article I, § 1 of the California Constitution. Defendants acts also violated federal statutes and regulations,  
22 including Federal Trade Commission Act (15 U.S.C. § 45 *et seq.*), HIPAA") (45 C.F.R. § 160.102), the  
23 HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards  
24 for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for  
25 the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts  
26 A and C and the other sections identified above. Plaintiff reserves the right to allege other violations of  
27 law committed by Defendants that constitute unlawful business acts or practices within the meaning of  
28 California Business & Professions Code sections 17200, *et seq.*

1 134. Defendants have also engaged in “unfair” business acts or practices. There are several  
2 tests that determine whether a practice that impacts consumers as compared to competitors is “unfair,”  
3 examining the practice’s impact on the public balanced against the reasons, justifications and motives of  
4 Defendants. Defendants’ conduct would qualify as “unfair” under any of these standards:

- 5 (a) does the practice offend an established public policy, which here are whether the practices  
6 at issue offend the policies of protecting consumers’ Medical Information by engaging in  
7 illegal practices, as reflected in California law and policy set forth above;
- 8 (b) balancing the utility of Defendants’ conduct against the gravity of the harm created by  
9 that conduct, including whether Defendants’ practices caused substantial injury to  
10 consumers with little to no countervailing legitimate benefit that could not reasonably  
11 have been avoided by the consumers themselves, and causes substantial injury to them; or
- 12 (c) is the practice immoral, unethical, oppressive, unscrupulous, unconscionable or  
13 substantially injurious to consumers.

14 135. The harm caused by Defendants’ failure to maintain adequate information security  
15 procedures and practices, including but not limited to failing to take adequate and reasonable measures  
16 to ensure their data systems were protected against unauthorized intrusions, failing to properly and  
17 adequately educate and train employees, failing to put into place reasonable or adequately protected  
18 computer systems and security practices to safeguard patients’ Medical Information, including access  
19 restrictions, multi-factor authentication and encryption, failing to have adequate privacy policies and  
20 procedures in place that did not preserve the confidentiality of the Medical Information, PHI and PII of  
21 Plaintiff and the Class members in their possession, failing to timely and accurately disclose the  
22 ransomware attack and resulting data breach to Plaintiff and Class members, and failing to protect and  
23 preserve confidentiality of Medical Information of Plaintiff and Class members against disclosure and/or  
24 release, outweighs the utility of such conduct and such conduct offends public policy, is immoral,  
25 unscrupulous, unethical, and offensive, and causes substantial injury to Plaintiff and Class members.

26 136. Defendants either knew or should have known that PHC’s data security and protection  
27 practices were inadequate to safeguard the Medical Information, PII and PHI of Plaintiff and Class  
28 members, deter hackers, and detect a ransomware attack and resulting data breach within a reasonable

1 time, even though the risk of a data breach or theft was highly likely, especially given Defendants had  
2 been on notice for almost a year of the potential for a Hive ransomware attack on its systems. The business  
3 acts and practices by Defendants for failure to keep confidential medical, demographic or personal data  
4 protected, encrypted and without sufficient security to be breached by an adverse third party did not meet  
5 all applicable standards of care and vigilance. Hundreds of thousands of individuals are now prime targets  
6 for fraud, extortion, or access to other completely private information that would never have been  
7 provided to Defendants if the patients or consumers knew how negligent or reckless Defendants would  
8 be in not protecting such deeply personal medical and financial information private.

9 137. These unlawful and unfair business acts or practices conducted by Defendants have been  
10 committed in the past and continue to this day. Defendants have failed to fully acknowledge the wrongful  
11 nature of their actions. Defendants have not corrected or publicly issued comprehensive corrective notices  
12 to Plaintiff and the Class members and may not have corrected or enacted adequate policies and  
13 procedures to protect and preserve confidentiality of medical and personal identifying information of  
14 Plaintiff and the Class in their possession.

15 138. As set forth above, Plaintiff and/or Class members have been injured in fact and lost  
16 money or property as a result of Defendants' unlawful and unfair business practices, having lost control  
17 over information about them that has a specific inherent monetary value that can be sold, bartered or  
18 exchanged.

19 139. Plaintiff and Class members have no other adequate remedy of law in that absent  
20 injunctive relief from the Court Defendants are likely to not fully redress the issues raised by their illegal  
21 and unfair business practices. Defendants have not announced any specific changes to their data security  
22 infrastructure, processes or procedures to fix the vulnerabilities in the electronic information security  
23 systems and/or security practices that permitted the Hive ransomware attack and resulting data breach to  
24 occur and go undetected, and thereby prevent further attacks, nor have they provided prompt and  
25 complete notice of the circumstances surrounding this breach as required by law. Pursuant to Business  
26 & Professions Code section 17203, Plaintiff seeks an order of this Court both for himself, members of  
27 the Class and for the benefit of the public for injunctive relief in the form of requiring Defendants to  
28 correct their illegal conduct, to prevent Defendants from repeating the illegal and wrongful practices as

1 alleged above and protect and preserve confidentiality of Medical Information in Defendants' possession  
2 that has been accessed, downloaded, exfiltrated, stolen, and viewed by at least one unauthorized third  
3 party because of Defendants' illegal and wrongful practices set forth above. Pursuant to Business &  
4 Professions Code section 17203, Plaintiff also seeks an order of this Court for injunctive relief in the  
5 form of prohibiting Defendants from continuing to refuse publicly issuing comprehensive direct and  
6 corrective notices. While not a claim for damages, Plaintiff will amend this claim to seek restitution if  
7 Defendants do not timely or adequately respond to the Notice of Violation and claims submitted by  
8 Plaintiff's counsel referenced above.

9 140. This action, if successful, will enforce an important right affecting the public interest and  
10 would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons and/or  
11 the general public. Private enforcement is necessary and places a disproportionate financial burden on  
12 Plaintiff in relation to Plaintiff's stake in the matter. Because this case is brought for the purposes of  
13 enforcing important rights affecting the public interest, Plaintiff also seeks the recovery of attorneys' fees  
14 and costs in prosecuting this action against Defendants under Code of Civil Procedure section 1021.5 and  
15 other applicable law.

## 16 **FIFTH CAUSE OF ACTION**

### 17 **Declaratory Relief**

18 141. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein.

19 142. A present and actual controversy exists between the parties. Defendants have failed to  
20 acknowledge the wrongful nature of their actions, have not sent affected patients complete and adequate  
21 data breach notices regarding the ransomware attack and data theft at issue herein nor offered adequate  
22 compensation or data monitoring, nor publicly issued comprehensive corrective notices. Based on their  
23 inadequate disclosures to date, there is also no reason to believe that Defendants have taken adequate  
24 measures to correct or enact adequate privacy policies and procedures to protect and preserve Plaintiff's  
25 and the Class members' Medical Information, PII and PHI in Defendants' possession.

26 143. Now that Defendants' insufficient information security is known to hackers, the Medical  
27 Information, PII and PHI in Defendants' possession is even more vulnerable to cyberattack.

28 144. Plaintiff and the Class members have no other adequate remedy of law in that absent

1 declaratory relief from the Court, Defendants are likely to not fully remedy the underlying wrong.

2 145. As described above, Defendants' actions have caused harm to Plaintiff and Class  
3 members. Further, Plaintiff and Class members are at risk of additional or further harm due to the  
4 exposure of their Medical Information, PII and PHI and Defendants' failure to fully address the security  
5 failings that lead to such exposure and provide adequate notice thereof.

6 146. Plaintiff and the Class members seek an order of this Court for declaratory, equitable  
7 and/or injunctive relief in the form of an order finding Defendants have failed and continue to fail to  
8 adequately protect Plaintiff's and the Class members' Medical Information, PII and PHI from release to  
9 unknown and unauthorized third parties, requiring Defendants to correct or enact adequate privacy  
10 policies and security measures to protect and preserve Plaintiff's and the Class members' Medical  
11 Information, PII and PHI in its possession, and requiring Defendants to publicly issue comprehensive  
12 corrective notices to Plaintiff, Class members and the public.

13 **PRAYER FOR RELIEF**

14 **WHEREFORE**, Plaintiff, both individually and on behalf of the Class and for the benefit of the  
15 public, pray for orders and judgment in favor of Plaintiff and against Defendants as follows:

- 16 A. Finding that this action satisfies the prerequisites for maintenance as a class action under  
17 Fed. R. Civ. Proc. 23 and certifying the Class defined herein;
- 18 B. Designating Plaintiff as a representative of the Class and his counsel as Class counsel;
- 19 C. Declaring Defendants' conduct in violation of the laws set forth above, including  
20 California Civil Code sections 56.10(a), 56.101, 1798.21, 1798.29, Business and  
21 Professions Code § 17200 *et seq.*, and Article I, § 1 of the California Constitution.
- 22 D. An order:
- 23 1. prohibiting Defendants from engaging in the wrongful and unlawful acts described  
24 herein;
  - 25 2. prohibiting Defendants from refusing to send all affected persons adequately  
26 comprehensive data breach notices regarding the ransomware attack and data theft  
27 at issue herein in the form required by law, offer more comprehensive credit  
28 monitoring services and publicly issue comprehensive corrective notices to

1 Plaintiff, Class members and the public;

- 2 3. prohibiting Defendants from failing to protect, including through encryption, all  
3 data collected through the course of their business operations in accordance with  
4 all applicable regulations, industry standards, and federal and state laws;
- 5 4. prohibiting Defendants from refusing to implement and maintain a comprehensive  
6 Information Security Program designed to protect the confidentiality and integrity  
7 of the Medical Information, PII and PHI of Plaintiff and the Class members;
- 8 5. prohibiting Defendants from refusing to engage independent third-party security  
9 auditors/penetration testers as well as internal security personnel to run automated  
10 security monitoring, database scanning and security checks and conduct testing,  
11 including simulated attacks, penetration tests, and audits on Defendants' systems  
12 on a periodic basis, and ordering Defendants to promptly correct any problems or  
13 issues detected by such third-party security auditors;
- 14 6. prohibiting Defendants from refusing to audit, test, and train security personnel  
15 regarding any new or modified procedures;
- 16 7. requiring Defendants to segment data by, among other things, creating firewalls  
17 and access controls so that if one area of Defendants' network is compromised,  
18 hackers cannot gain access to other portions of Defendants' systems;
- 19 8. prohibiting Defendants from refusing to establish an information security training  
20 program that includes at least annual information security training for all  
21 employees, with additional training to be provided as appropriate based upon the  
22 employees' respective responsibilities with handling personal identifying  
23 information, as well as protecting the personal identifying information of Plaintiff  
24 and Class members and infiltration of Defendants' computer system by phishing  
25 processes by using such steps such as multi-factor authentication;
- 26 9. prohibiting Defendants from refusing to routinely and continually conduct internal  
27 training and education, and inform internal security personnel how to immediately  
28 identify and contain a ransomware attack or data breach when it occurs and what



1 to do in response to a breach; and,

2 10. prohibiting Defendants from refusing to implement, maintain, regularly review,  
3 and revise as necessary a threat management program designed to appropriately  
4 monitor Defendants' information networks for threats, both internal and external,  
5 and assess whether monitoring tools are appropriately configured, tested, and  
6 updated;

7 E. Awarding Plaintiff's counsel reasonable attorneys' fees and non-taxable expenses;

8 F. Awarding Plaintiff's costs;

9 G. Awarding pre- and post-judgment interest at the maximum rate permitted by applicable  
10 law; and,

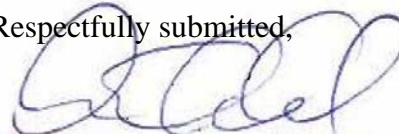
11 H. Granting such further relief as the Court deems just.

12 **JURY DEMANDED**

13 Plaintiff demands a trial by jury on all issues so triable.

14 Dated: May 27, 2022

15 Respectfully submitted,



16 **WHATLEY KALLAS, LLP**

17 Alan M. Mansfield, SBN: 125998  
18 1 Sansome Street, 35th Floor  
19 PMB #131  
20 San Francisco, CA 94104

21 16870 W. Bernardo Drive  
22 Suite 400  
23 San Diego, CA 92127  
24 Phone: (619) 308-5034  
25 Fax: (888) 341-5048  
26 Email: amansfield@whatleykallas.com

27 **WHATLEY KALLAS, LLP**

28 Joe R. Whatley, Jr. (*Pro Hac Vice application to  
be filed*)  
jwhatley@whatleykallas.com  
Edith M. Kallas (*Pro Hac Vice application to be  
filed*)  
ekallas@whatleykallas.com  
Patrick J. Sheehan (*Pro Hac Vice application to be  
filed*)

1 152 W. 57th Street, 41st Floor  
2 New York, NY 10019  
3 Tel: (212) 447-7060  
4 Fax: (800) 922-4851

5 **JANSSEN MALLOY LLP**  
6 Megan A. Yarnall, SBN: 275319  
7 730 Fifth Street  
8 Eureka, CA 95501  
9 Phone: (707) 445-2071 ext. 223  
10 Fax: (707) 445-8305  
11 Email: myarnall@janssenlaw.com

12 **APRIL M. STRAUSS, A PC**  
13 April M. Strauss, SBN: 163327  
14 2500 Hospital Drive, Bldg. 3  
15 Mountain View, CA 94040  
16 Phone: (650) 281-7081  
17 Email: astrauss@sfaclp.com

18 **DOYLE APC**  
19 William J. Doyle, SBN: 188069  
20 550 West B Street  
21 4<sup>th</sup> Floor  
22 San Diego, CA 92101  
23 Phone: (619) 736-0000  
24 Fax: (619) 736-1111  
25 Email: bill@doyleapc.com

26 *Attorneys for Plaintiff*  
27  
28

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

John Doe, on behalf of himself and all others similarly situated and for the benefit of the general public,

(b) County of Residence of First Listed Plaintiff Elko County, Nevada (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

Alan M. Mansfield, Whatley Kallas, LLP, 1 Sansome Street, 35th Floor, PMB #131, San Francisco, CA 94104 (619) 308-5034

DEFENDANTS

Partnership HealthPlan of California, and Does 1 through 10, inclusive

County of Residence of First Listed Defendant (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff 3 Federal Question (U.S. Government Not a Party) 2 U.S. Government Defendant 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship and incorporation status.

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, HABEAS CORPUS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding 2 Removed from State Court 3 Remanded from Appellate Court 4 Reinstated or Reopened 5 Transferred from Another District (specify) 6 Multidistrict Litigation-Transfer 8 Multidistrict Litigation-Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. 1332(d)

Brief description of cause:

Class Action alleging Unauthorized, Unprivileged Disclosure to a Third-Party of Nonpublic Medical Information

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P.

DEMAND \$ 5,000,000.00 Exceeds

CHECK YES only if demanded in complaint: JURY DEMAND: X Yes No

VIII. RELATED CASE(S), IF ANY (See instructions):

JUDGE Canning, Humboldt Co Sup Ct

DOCKET NUMBER

Cal Sup Ct, CV-22-00606 and CV-22-00719

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only)

SAN FRANCISCO/OAKLAND

SAN JOSE

X EUREKA-MCKINLEYVILLE

DATE 05/27/2022

SIGNATURE OF ATTORNEY OF RECORD

/s/ Alan M. Mansfield

**INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44**

**Authority For Civil Cover Sheet.** The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I. a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
  - b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the “defendant” is the location of the tract of land involved.)
  - c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section “(see attachment).”
- II. Jurisdiction.** The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an “X” in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- (1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.
  - (2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an “X” in this box.
  - (3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
  - (4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an “X” in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. Origin.** Place an “X” in one of the six boxes.
- (1) Original Proceedings. Cases originating in the United States district courts.
  - (2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.
  - (3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
  - (4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
  - (5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
  - (6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.
  - (8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket. Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an “X” in this box if you are filing a class action under Federal Rule of Civil Procedure 23. Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction. Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.
- IX. Divisional Assignment.** If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: “the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated.”
- Date and Attorney Signature.** Date and sign the civil cover sheet.

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Partnership HealthPlan of California Hit with Class Action Following Hive Ransomware Attack](#)

---