WHATLEY KALLAS, LLP
Alan M. Mansfield, SBN: 125998
16870 W. Bernardo Drive
Suite 400
San Diego, CA 92127
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]

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF HUMBOLDT

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 25, inclusive,

Defendants.

Case No. CV2200606 **Fax File**

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

Plaintiff John Doe ("Plaintiff"),[1] brings this action on behalf of himself and all others similarly situated and for the benefit of the general public against Defendant Partnership HealthPlan of California ("PHC") and DOES 1–25, inclusive (collectively referred to herein as "Defendants"). Plaintiff, through his undersigned counsel, alleges the following based on personal knowledge as to allegations regarding Plaintiff, and on information and belief as to all other allegations.

SUMMARY OF THE ACTION

1. This action arises from the failure by PHC to adequately secure the private, personal medical information of Plaintiff and all others similarly situated who are current residents of California and enrolled or previously enrolled in PHC's health care service plans. As detailed more fully below, in March 2022 PHC was subject to a ransomware attack and accompanying data breach and theft by the Hive ransomware group ("Hive"). When compared to the data reported by HHS Office of Civile Rights for the last 24 months, this would be the 2nd largest health plan data breach in the United States. The Hive group reported that, on or about March 19, 2022, it had gained access to Defendant PHC's computer network, deployed malware that encrypted data in PHC's servers, and had acquired copies of 850,000 personal unique records related to PHC enrollees, and over 400 gigabytes of enrollees' personal information stored on Defendant PHC's computer network servers. PHC has reported that, "[i]n the initial period after the March 19 system disruption, PHC operations were at a standstill." PHC failed to take steps necessary to prevent such an attack and has refused to date to notify victims of this ransomware attack that their personal information was improperly accessed and stolen.

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

3. In California, the protection of personal privacy is of paramount importance. Article 1, section 1 of the California Constitution guarantees consumers their right to privacy. In addition, as recognized by the California Legislature, the use of sophisticated computer information technology has

[1] Due to the sensitive nature of this action, Plaintiff has chosen to file under a pseudonym. (*See, e.g., Jane Doe 8015 v. Sup. Ct.* (2007) 148 Cal.App.4th 489).

greatly magnified the potential risk to individual privacy that occurs from the maintenance of personal information by entities such as Defendants, necessitating that the maintenance of personal information is subject to strict limits governed by numerous California statutes.[2]

4. Medical information in California is considered to be among the most sensitive private personal information available.[3] "Medical Information" is defined by California's Confidential Medical Information Act, Cal. Civ. Code sections 56, *et seq*. ("CMIA") as:

> any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment.
>
> "Individually identifiable" means that the Medical Information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or Social Security Number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual.[4]

5. "Medical Information", for purposes of this Complaint, thus refers to the above definition, and encompasses both Personal Health Information ("PHI"), and Personally Identifiable Information ("PII"), including Social Security Numbers associated with individual health records within PHC's computer systems.

6. Since Medical Information encompasses such personal and revealing information, it is highly valued as a gateway to medical identity theft[5] and more general identity theft.[6] Medical Information has been found to command up to $1,000 per individual record on the dark web.[7] Thus, organizations such as Defendants who are entrusted with this most sensitive and valuable data have a non-delegable duty to take particularly special care to maintain up-to-date information security practices and keep apprised of industry-related threats as they arise. The threat from the Hive group of a ransomware attack was reasonably foreseeable to Defendants, as health care companies had been warned for almost a year of the potential for such an attack on their computer systems.

---

[2] See Cal. Civil Code § 1798.1(b) & (c).
[3] *See, e.g.,* Cal. Civ. Code § 1798.140(ae)(2)(B) (as amended by Proposition 24) (defining health information as sensitive data).
[4] Cal. Civ. Code § 56.05(i).
[5] R. Kam, *et al, Medical Identity Theft: A Deadly Side Effect of Healthcare Data Breaches*, ID Experts (2017).
[6] Identity Theft Resource Center, *Data Breaches in the Healthcare Industry Continue Due to Availability of Valuable Information* (8/11/2020).
[7] M. Yao, *Your Electronic Medical Records Could be Worth $1,000 to Hackers*, Forbes (4/18/17).

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

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

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

> The Legislature hereby finds and declares that persons receiving health care services have a right to expect that the confidentiality of individual identifiable Medical Information derived by health service providers be reasonably preserved. It is the intention of the Legislature in enacting this act, to provide for the confidentiality of individually 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 provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization [. . .]." (Cal. Civ. Code § 56.10(a).) Defendants' actions permitted the disclosure of the Medical Information at issue here to unauthorized third parties.

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

12. Unfortunately for Plaintiff and other similarly situated individuals who either are or were enrolled with PHC, their personal information and sensitive Medical Information was not secured in the manner required under California law that would prevent such unauthorized access. What's worse, despite Defendants' obligations under the law to promptly notify affected individuals so they can take appropriate action, Defendants have failed to promptly provide such notice in the most expedient time possible and without unreasonable delay or advise affected individuals that their Medical Information may have been illegally misappropriated.

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

14. The remedies provided for under Civil Code Section 56.36(b) allow private litigants to bring an action against an entity that has permitted the negligent release of confidential information or records or that failed to create, maintain, preserve, or store Medical Information in a manner that preserves its confidentiality to seek injunctive relief and, among other remedies, statutory damages of one thousand dollars ($1,000). In order to recover under this paragraph, it is not necessary that the plaintiff suffered or was threatened with actual damages. (Cal. Civ. Code § 56.36(b)(1).) These remedies are in addition to any other remedies available at law. (Cal. Civ. Code § 56.36(b).) Plaintiff has submitted a demand for the payment of damages to Defendants. Plaintiff only seeks injunctive and equitable relief at this time but reserves the right to seek damages if Defendants do not timely and fully respond to

Plaintiff's claim.

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

16. Defendants disregarded the rights of Plaintiff and members of the Class by negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and the Class members' personal and Medical Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding data access and encryption, even for internal use, as well as appropriate procedures that would prevent such intrusions through methods such as phishing, such as multi-factor authentication. As a result, the PHI, PII and Medical Information of hundreds of thousands of PHC enrollees was compromised through disclosure to unknown and unauthorized third parties. While Defendants have yet to confirm the nature of the data that was taken, reportedly this data includes, but is potentially not limited to, enrollees' full names, dates of birth, addresses, and Social Security Numbers, as well as likely their associated medical conditions, health insurance provider information, public health program participant information, and program eligibility dates.

17. Plaintiff and all other similarly situated enrollees in PHC's programs face a long-term battle against identity theft if their full names, Social Security Numbers, dates of birth, addresses, health information, and other contact information were contained in this unauthorized access and exfiltration. Plaintiff and the Class members have a continuing interest in ensuring that their information is and remains safe. As shown by PHC's total shutdown of its system for close to a month, stolen Medical Information can be used to interrupt important medical services. This presents an imminent and impending continuing risk for Plaintiff and Class members, particularly where PHC refuses to disclose any details of the ransomware attack. Plaintiff and the Class are thus entitled to injunctive and other equitable relief. PHC's failure to adequately protect the nonpublic personal and Medical Information in their possession has likely caused, and will continue to cause, substantial harm and injuries to Plaintiff and Class members.

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

JURISDICTION AND VENUE

19. This Court has jurisdiction over this matter pursuant to California Code of Civil Procedure section 410.10 because the acts set forth in this Complaint took place in California, Plaintiff and Class members are all current residents and citizens of California, and Defendants conduct either all or a vast majority of their business in California and hold themselves out as a California state agency.

20. Venue is proper in Humboldt County pursuant to California Code of Civil Procedure section 395 and 395.5 because a substantial part of the events and omissions giving rise to the claims occurred in this County as set forth herein, the Plaintiff resides here, and Defendant has significant operations in this County. In addition, Civil Code Section 1798.49 provides that claims under the California Information Practices Act of 1977 ("Cal IPA") can be filed in the County where the Plaintiff resides or where the records are located, both of which are in this County.

PARTIES

21. On personal knowledge, Plaintiff John Doe is a citizen and current resident of the State of California and is enrolled in PHC and has been for several years. Plaintiff resides in Humboldt County, California. Plaintiff and his family use medical services in this County, which are paid for in whole or in part by PHC. Plaintiff, like each member of the Class, provided Defendants with individually identifiable information and Medical Information, as defined by Civil Code section 56.05(i), in order to receive health care benefits through Defendants' health insurance network. Many of his and his family's medical records are located in this County. Plaintiff works as a technician in the medical field and understands the importance of protecting the confidentiality of Medical Information. The protection of such information for both him and his family from unauthorized disclosure is thus important and material to him. Plaintiff has experienced fear, anxiety, and worry caused by the unauthorized disclosure of Medical Information by PHC since he became aware of it. He remains concerned about the status of this information as he has not received any notice from PHC confirming this ransomware attack, or the steps he should take to protect both him and his family, particularly in terms of sensitive Social Security Numbers and Medical Information.

22. Plaintiff and his family's medical history, mental or physical condition, or treatment, including diagnosis and treatment dates, was created, maintained, preserved, and stored onto Defendants' computer network. Such Medical Information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as name, date of birth, address, and Social Security Number, and additionally likely also contained medical record number, insurance provider, electronic mail address, telephone number, or other information that, alone or in combination with other publicly available information, reveals Plaintiff's identity. Through the exfiltration of such data, he has been injured in fact and lost money or property as a result of Defendants' misconduct in having his Medical Information likely disclosed to and stolen by third parties without his authorization, and the confidentiality and integrity of his Medical Information breached, lost, not preserved, and not protected.

23. Defendant PHC identifies itself as a government agency subject to the California Information Practices Act of 1977 that, among other things, manages Med-Cal beneficiaries who reside in various Northern California counties, including Humboldt County. PHC operates a managed health care system designed provide health care delivery to individuals in Del Norte, Humboldt, Lake, Lassen, Marin, Mendocino, Modoc, Napa, Trinity, Shasta, Siskiyou, Solano, Sonoma, and Yolo Counties in Northern California. PHC is organized as a health insuring organization under California law. Defendant maintains a regional office in Eureka, California. PHC claims to currently serve approximately 600,000 members. PHC is considered a "covered entity" for purposes of HIPAA.

24. The true names, roles, and capacities in terms of their involvement in the wrongdoing at issue, whether individual, corporate, associate, or otherwise, of Defendants named as DOES 1 through 25, inclusive, are currently unknown to Plaintiff and, therefore, are named as Defendants under fictitious names pursuant to California Code of Civil Procedure Section 474. Plaintiff will identify these Defendants' true identities and their involvement in the wrongdoing at issue if and when they become known.

25. Defendants' conduct described herein including reviewing, approving, or ratifying the conduct at issue, was undertaken either directly by PHC or as an agent, servant, contractor, or employee of PHC pursuant to California Civil Code Section 1798.19, and/or was performed within the course and

scope of their authority, agency, or employment. Defendants are thus jointly and severally responsible, in whole or in part, for the conduct, damages, and injuries alleged herein.

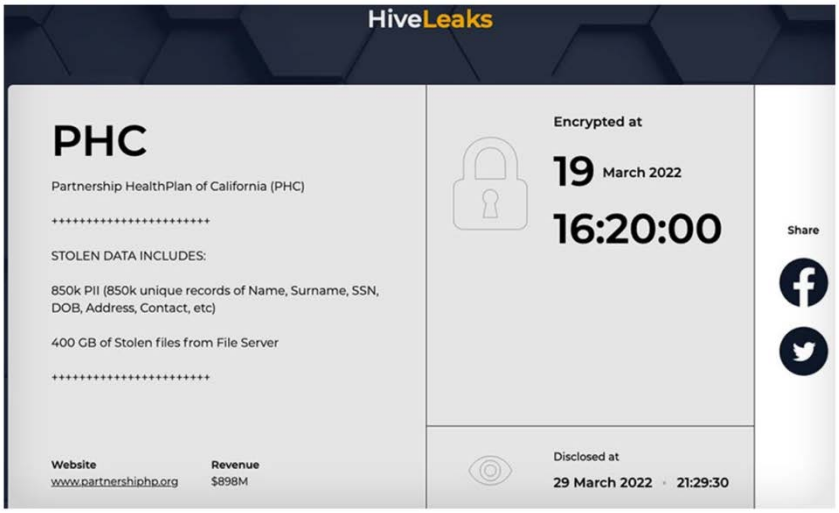
FACTUAL ALLEGATIONS

A. THE NATURE OF THE RANSOMWARE ATTACK.

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

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

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



29. On or about March 30, 2022, PHC shut down their entire patient-interfacing website. Critically, it did not tell its members it had been subject to a ransomware attack, that over 850,000 unique

records had been accessed and 400 Gigabytes of information had been stolen from PHC's file servers so that consumers could protect themselves. Rather, PHC uploaded the following message that cryptically read, in relevant part:

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

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

31. On or about April 15, 2022, PHC reported that it had restored its website functionality, only acknowledging there had been a "detection of anomalous activity within areas of the organization's network." However, PHC has not, as of the time of this filing, informed its members about this ransomware event, nor suggested they take any precautions to prevent identity theft stemming from the access and disclosure of their personal and Medical Information, nor offered them any compensation. Defendants have failed to notify affected California residents about the breach in the security of their personal data at all, and in the timeframe required under California Civil Code Section 1798.29(a).

32. On or about April 29, 2022, Plaintiff, through his counsel, sent a Notice of Violation to PHC and to the State of California, requesting, in part, that they provide immediate notice of this data breach to both himself and all similarly situated PHC members as to the scope and nature of this attack. The Notice notes that doing so is of particular immediate concern, as Plaintiff and others do not know what steps to take to protect their PII, and in many instances may not know that a data breach has even taken place. As of the filing of this Complaint, PHC has not responded to this request. 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 Plaintiff's claim for damages, on behalf of both himself and all others similarly situated.

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

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

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

35. Specifically, as early as July 30, 2021, the U.S. Department of Health and Human Services ("HHS") issued an alert about the Hive group and its potential threat to healthcare organizations.[8] Referring to it as "nightmare," HHS recommended that healthcare organizations ensure they review the list of recommended mitigations in the Alert and promptly apply them to impacted systems in their infrastructure.[9]

36. On August 25, 2021, the HHS Cybersecurity Program published another Alert entitled **Indicators of Compromise Associated with Hive Ransomware.**[10] The Alert was also widely circulated and reported on by the media after its release.[11] HHS in particular noted that Hive had targeted entities in the Healthcare and Public Health Sector. The Alert, issued in conjunction with the FBI, described how the Hive group was operating, linked to an FBI Flash Alert that contained technical details about the Hive ransomware group's methods, sample ransom letters, and recommendations to detect, avoid and recover

[8] *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 (last accessed 5/3/22).
[9] *Id.*
[10] 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).
[11] *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);

from Hive's intrusions.[12] The Alert contains a list of specific, technical indicators to immediately advise companies such as PHC that a system has been compromised by the Hive ransomware group, recognizing that awareness of these indicators could allow for detection during an attack and can help contain or minimize its impact.[13]

37. According to the FBI Alert,

> "Hive ransomware uses multiple mechanisms to compromise business networks, including phishing emails with malicious attachments to gain access and Remote Desktop Protocol (RDP) to move laterally once on the network."
>
> "After compromising a victim network, Hive ransomware actors exfiltrate data and encrypt files on the network. The actors leave a ransom note in each affected directory within a 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.'"[14]

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

> "Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. ***Paying the ransom also does not guarantee that a victim's files will be recovered***."[15]

39. The FBI Flash Alert also contained recommended mitigations:

- Back-up critical data offline.
- Ensure copies of critical data are in the cloud or on an external hard drive or storage device.
- Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.
- Use two-factor authentication with strong passwords, including for remote access services.
- 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.

---

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

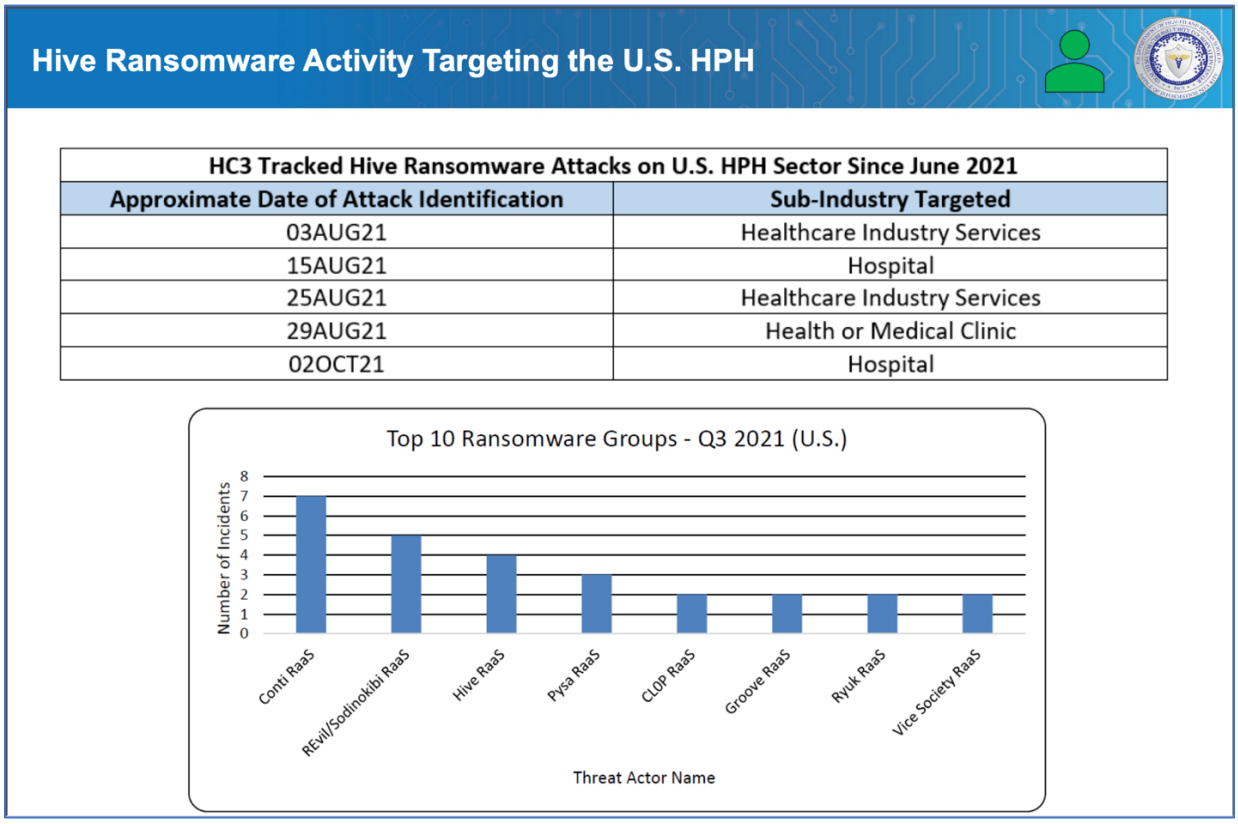
[13] HHS Cybersecurity Program HC3: Analyst Note (April 18, 2022), https://www.hhs.gov/sites/default/files/hive-ransomware-analyst-note-tlpwhite.pdf (last accessed 5/3/21).

[14] FBI Flash TLP White, n.12 *supra*, at 1.

[15] *Id*., at 6 (emphasis added). This admonition comports with the trend noted by the Comparitech, which specializes in cyber security and privacy online, who also notes that "[t]here has also been a growing trend of double-extortion attempts in which hackers not only lock computers with a message demanding a ransom but also contact victims with proof of the data collected." https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

- Install and regularly update anti-virus or anti-malware software on all hosts.[16]

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



41. 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.[20]

---

[16] *Id.* at 7-8. The August Alert also contains links to additional resources to prevent, protect and respond to ransomware events.
[17] *See*, HHS Cybersecurity Program Hive Ransomware (10/21/21), https://www.hhs.gov/sites/default/files/hive-ransomware-tlpwhite.pdf (last accessed 5/3/22).
[18] *Id.*
[19] *Id.* at 8.
[20] *Id.* at 9.

42. HHS has analyzed Hive's operations to be "standard practice amongst ransomware operators."[21] As the HHS Analyst points out:

> When defending against Hive or any other ransomware variant, there are standard practices that should be followed. *Prevention is always the optimal approach*. This includes but is not limited to the following:
>
> - Use two-factor authentication with strong passwords – this is especially applicable for remote access services such as RDP and VPNs.
> - Sufficiently backing up data, especially the most critical, sensitive and 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 two different forms of media, with one of them stored offline.
> - Continuous monitoring is critical, and should be supported by a constant input of threat data (open source and possibly proprietary as well)
> - An active vulnerability management program must be comprehensive in scope and timely in implementation of the latest software updates. It should apply to traditional information technology infrastructure as well as any medical devices or equipment that is network-connected.
> - Endpoint security should be comprehensive in scope and updated with the latest signatures/updates aggressively.[22]

43. Yet despite numerous attempts on the part of the federal government to inform healthcare organizations, like PHC, of the threat posed by ransomware attacks in general and Hive in particular, and

[21] HHS Cybersecurity Program HC3: Analyst Note, *supra*.
[22] *Id. (emphasis added).*

despite having almost a year from their attack to prepare and prevent such an attack, PHC was negligent and did not adequately prepare for this wholly foreseeable event, allowing extremely sensitive data to be accessed, viewed and stolen by the Hive group.

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

45. Defendants either knew, or reasonably should have known, the importance of safeguarding the Medical Information entrusted to them and of the foreseeable consequences if their computer network was breached. Defendants failed, however, to take adequate measures to prevent the Hive ransomware attack. Defendants were on notice that they should have and could have prevented this attack by properly securing and encrypting the Medical Information, PII and PHI of Plaintiff and the Class members and taking the steps outlined above to prevent infiltration by methods such as phishing by, for example using multi-factor authentication methods. Defendants could also have destroyed data of former enrollees that was no longer useful, especially outdated data.

46. The American Medical Association ("AMA") has previously warned healthcare companies about the importance of protecting their patients' confidential information:

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

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

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

the issuance of that report. [24]

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

49. For example, Universal Health Services experienced a cyberattack on September 29, 2020, that appears similar to the ransomware attack on Defendants. As a result of this attack, Universal Health Services suffered a four-week outage of its systems, which caused as much as $67 million in recovery costs and lost revenue.[27] Similarly, on or about May 1, 2021, Scripps Healthcare in San Diego suffered a cyberattack, an event that effectively shut down critical health care services for a month and left numerous patients unable to speak to physicians or access vital medical and prescription records, just as happened here.[28] A couple of months later in July 2021, University of California San Diego Health suffered a similar attack.[29]

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

51. Yet, despite the prevalence of public announcements of these data breach and data security

---

[24] 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)

[25] Critical Insight, *Health Breach Report July-Dec 2021* (2022), p. 3.

[26] *Id.* at 6.

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

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

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

compromises, Defendants failed to take appropriate steps to protect Plaintiff's and Class members' Medical Information from being compromised and have failed to notify such persons that such an attack had taken place and the nature of the exfiltrated data.

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

52. Defendants are required by the Cal IPA, the CMIA and various other laws and regulations to protect Plaintiff's and Class members' Medical Information and to handle notification of any breach in accordance with applicable breach notification statutes. Defendants also needed to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems. Failing to do so results in acts of negligence *per se* by Defendants. These duties are established in numerous California statutes, including California Civil Code Sections 56.101, 1798.21, and 1798.26.

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

54. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

> "Electronic protected health information" is defined as "individually identifiable health information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

55. HIPAA's Security Rule requires Defendants to: (a) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; (b) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (c) Protect against any reasonably anticipated uses or

disclosures of such information that are not permitted; and (d) Ensure compliance by their workforce.

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

57. The ransomware attack on Defendants, particularly in light of the information received by them almost a year before the attack, establishes they did not comply with these Rules. This attack 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:

(a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendants create, receive, maintain, and transmit, in violation of 45 C.F.R. section 164.306(a)(1);

(b) Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);

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

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

(e) Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);

(f) Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually

identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);

(g) Failing to ensure compliance with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. section 164.306(a)(4);

(h) Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, *et seq.*;

(i) Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and

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

58. Defendants also violated the duties applicable to them under the Federal Trade Commission Act (15 U.S.C. § 45 *et seq.*) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC pursuant to that Act has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.[30]

59. As established by these laws, Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Medical Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants also owed a duty to Plaintiff and Class members to provide reasonable security in compliance with industry standards and state and federal requirements, and to ensure that their computer systems, networks, and protocols adequately protected this Medical Information and were not exposed to infiltration. This also included a duty to Plaintiff and the Class members to design, maintain, and test their computer systems to ensure that the Medical Information in their possession was adequately

[30] *See, e.g., FTC v. Wyndham Worldwide Corp.*, (3d Cir. 2015) 799 F.3d 236.

secured and protected; to create and implement reasonable data security practices and procedures to protect the Medical Information in their possession and avoid access to their systems through processes such as phishing, including adequately training employees and others who accessed information within their systems on how to adequately protect Medical Information and avoid permitting such infiltration such as by use of multi-factor authentication; to implement processes that would detect a breach of their data security systems in a timely manner and to act upon data security warnings and alerts in a timely fashion; to disclose if their computer systems and data security practices were inadequate to safeguard individuals' Medical Information from theft; and to disclose in a timely and accurate manner when data breaches or ransomware attacks occurred.

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

61. As a direct and proximate result of Defendants' actions, inactions, omissions, breaches of duties and want of ordinary care that directly and proximately caused or resulted in the ransomware attack and the resulting data breach, Plaintiff and Class members have suffered and will continue to suffer damages and other injury and harm in the form of, *inter alia*, (a) present, imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud -- risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (b) invasion of privacy, (c) breach of the confidentiality of their Medical Information, (d) deprivation of the value of their PHI, for which there is a well-established national and international market, as well as statutory damages to which they are entitled even without proof of access or actual damages; (e) the financial and temporal

cost of monitoring their credit reports, (f) increased risk of future harm, and/or (g) have suffered fear, anxiety, and worry caused by the unauthorized release of their Medical Information, all resulting in a loss of money or property related to Defendants' misconduct.

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

62. It is well known that Medical Information is a valuable commodity[31] and the frequent target of hackers, such that Plaintiff and Class members would lose money or property if their data was permitted to be improperly accessed or stolen.

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

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

---

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

[32] Federal Trade Commission, What To Know About Identity Theft, https://consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed 5/3/22).

[33] Janelle Stecklein, *Director: 64,000-plus fraudulent unemployment claims 'mitigated'*, The Duncan Banner (June 24, 2020), 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).

over the previous 4 years.[34]

65. According to Experian, one of the three major credit bureaus, medical records can be worth up to $1,000 per person on the dark web, depending upon completeness.[35] PII and PHI can be sold at a price ranging from approximately $20 to $300.[36]

66. Medical identify theft can also result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences since if a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[37]

67. The Ponemon Institute found that medical identity theft can cost victims an average of $13,500 to resolve per incident, and that victims often have to pay off the imposter's medical bills to resolve the breach.[38]

68. In another study by the Ponemon Institute in 2015, 31% of medical identity theft victims lost their healthcare coverage as a result of the incident, while 29% had to pay to restore their health coverage, and over half were unable to resolve the identity theft at all.[39]

69. Once PHI, PII and Medical Information is stolen, particularly such as membership identification numbers or Social Security Numbers, fraudulent use of that information and damage to victims may continue for years, as the fraudulent use of such data resulting from the attack may not come

---

[34] *See*, Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web* (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).

[35] *Id.*

[36] https://www.privacyaffairs.com/dark-web-price-index-2021/

[37] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, (2/7/14), https://khn.org/news/rise-of-indentity-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).

[38] Brian O'Connor, Healthcare Data Breach: What to Know About Them and What to Do After One, 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).

[39] 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 (last accessed 5/3/22).

to light for years. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches: "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[40] The ramifications of Defendants' failure to keep the Medical Information in question secure from attack and then not advise affected persons of all the relevant facts is thus not temporary but long lasting, as the fraudulent use of that information and damage to victims may continue for years. That is one of the reasons providing prompt notice to consumers as expeditiously as possible is necessary, so they can take actions to protect themselves. Yet Defendants are still refusing to even acknowledge that a ransomware and resulting data breach took place, let alone providing comprehensive notice in the most expedient time possible and without unreasonable delay, as required under California law.

CLASS ALLEGATIONS

70. Plaintiff, on behalf of himself and all others similarly situated, brings this action pursuant to California Code of Civil Procedure Section 382. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements for class certification.

71. The proposed class ("Class") is defined as:

> All current California citizens and residents who are present or former enrollees of PHC's health care service plans and whose information was accessed and released or disclosed as a result of the Hive ransomware attack in or about March, 2022.

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

73. The members of the Class are sufficiently numerous such that joinder of all Class members is impracticable. The proposed Class contains past or current PHC members who had approximately 850,000 unique records improperly accessed or taken.

74. Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual Class members. The factual bases underlying Defendants'

[40] *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).

misconduct is common to all Class members and represents a common thread of unlawful and negligent conduct, resulting in injury to all members of the Class. These common legal and factual questions include the following:

(a) Whether Defendants implemented and maintained reasonable security practices and procedures appropriate to protect Plaintiff's and Class members' Medical Information from unauthorized access, destruction, use, theft, modification, or disclosure;

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

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

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

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

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

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

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

(i) Whether Plaintiff and the Class are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the ransomware attack and Defendants'

failure to provide notice thereof, and the scope of such relief.

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

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

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

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

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the Information Practices Act of 1977

Cal. Civ. Code § 1798 *et seq*.

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

80. Cal. Civ. Code section 1798.21 requires agencies of the State of California "to ensure the

security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury." Defendant PHC has identified itself as an agency subject to the provisions of the Cal IPA.

81. Cal. Civ. Code section 1798.21 also requires agencies of the State of California "to establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance" with the Cal IPA.

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

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

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

85. A data breach notification under the Cal IPA must meet specific content and format requirements as set forth in Civil Code section 1798.29(d), designed to call attention to the nature and

the significance of the information it contains and including, but not limited to the types of personal information reasonably believed to have been the subject of the breach, the date of the breach, a general description of the data breach incident, and the toll-free numbers and addresses of the major credit reporting agencies, if as here the breach exposed a Social Security Number or California identification card number.

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

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

(a) Defendants requested and came into possession of Plaintiff's and Class members' personal and Medical Information as a state agency to accomplish the agency's function as a health care service plan and had a statutory duty to exercise reasonable care in preserving the security and confidentiality of this information.

(b) Plaintiff and Class members, as enrollees in PHC's programs, had their personal and Medical Information negligently stored within Defendants' databases.

(c) Defendants were entrusted with Plaintiff's and Class members' personal and Medical Information, and therefore were required "to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury."

(d) Defendants were required to "establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance" with the Cal IPA.

(e) Defendants failed to ensure the security and confidentiality of Plaintiff's and Class members' records containing Medical Information.

(f) Defendants failed to protect Plaintiff's and Class members' records containing Medical Information against anticipated threats or hazards to their security or integrity, which could result in injury by failing to protect against the known Hive ransomware attack affecting those records in March 2022, as described above.

This attack was a threat or hazard to the security and/or integrity of that information that should have been anticipated by Defendants as having the potential to cause injury.

(g) Defendants failed to "establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance" with the Cal IPA, as evidenced by its failure to prevent or promptly identify the Hive ransomware attack affecting Plaintiff's and Class members' records in March 2022, as described above.

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

88. As a result of Defendant's failure to comply with and/or ensure compliance with the Cal IPA, Plaintiff and members of the Class have suffered injury.

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

90. Plaintiff seeks injunctive relief, fees and costs of suit as permitted by this statute.

SECOND CAUSE OF ACTION

Violation of the Confidentiality of Medical Information Act

Cal. Civ. Code § 56 *et seq*.

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

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

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

unauthorized third parties, in violation of this Section.

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

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

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

97. Plaintiff and members of the Class are "Patients" as defined by Cal. Civ. Code section 56.05(j).

98. The information at issue in this action is "Medical Information" as that term is defined by section 56.05(i) of the CMIA.

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

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

101. Since the Hive ransomware group was able to identify the contents of the 400 gigabytes of information it stole from PHC, as well as publicly reporting that the data stolen from PHC also included 850,000 PII such as "unique records of Name, Surname, SSN, DOB, Address, Contact, etc," the Hive

ransomware group necessarily viewed the data at issue herein and the confidentiality and integrity of that data was breached, lost, not preserved, and not protected by Defendants.

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

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

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

105. In violation of the CMIA, PHC's electronic health record systems or electronic medical record systems did not protect and preserve the integrity of Plaintiff's and Class members' Medical Information.

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

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

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

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

110. If Defendants do not timely respond to Plaintiff's claims for payment of damages

submitted prior to the initiation of this action, Plaintiff will amend this Complaint to seek actual damages, statutory damages of $1,000 per Class member and punitive damages of $3,000 per Class member.

THIRD CAUSE OF ACTION

Invasion of Privacy

California Constitution, Article I, Section 1

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

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

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

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

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

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

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

118. The intrusion at issue was into a place or thing, which was private and is entitled to be private. Plaintiff and Class members disclosed their Medical Information, PII and PHI to Defendants as part of Plaintiff's and Class members' relationships with Defendants, but privately and with the intention that the Medical Information, PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such

information would be kept private and would not be disclosed without their authorization.

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

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

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

122. As a proximate result of the above acts and omissions of Defendants, the Medical Information, PII and PHI of Plaintiff and Class members was disclosed to third parties without authorization, causing Plaintiff and Class members to suffer injuries and damages in an amount according to proof.

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

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

FOURTH CAUSE OF ACTION

Violation of the Unfair Competition Law

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

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

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

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

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

(a) does the practice offend an established public policy, which here are whether the practices at issue offend the policies of protecting consumers' Medical Information by engaging in illegal practices, as reflected in California law and policy set forth above;

(b) balancing the utility of Defendants' conduct against the gravity of the harm created by that conduct, including whether Defendants' practices caused substantial injury to consumers with little to no countervailing legitimate benefit that could not reasonably have been avoided by the consumers themselves, and causes substantial injury to them; or

(c) is the practice immoral, unethical, oppressive, unscrupulous, unconscionable or substantially injurious to consumers.

129. The harm caused by Defendants' failure to maintain adequate information security

procedures and practices, including but not limited to failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions, failing to properly and adequately educate and train employees, failing to put into place reasonable or adequately protected computer systems and security practices to safeguard patients' Medical Information, including access restrictions, multi-factor authentication and encryption, failing to have adequate privacy policies and procedures in place that did not preserve the confidentiality of the Medical Information, PHI and PII of Plaintiff and the Class members in their possession, failing to timely and accurately disclose the ransomware attack and resulting data breach to Plaintiff and Class members, and failing to protect and preserve confidentiality of Medical Information of Plaintiff and Class members against disclosure and/or release, outweighs the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous, unethical, and offensive, and causes substantial injury to Plaintiff and Class members.

130. Defendants either knew or should have known that PHC's data security and protection practices were inadequate to safeguard the Medical Information, PII and PHI of Plaintiff and Class members, deter hackers, and detect a ransomware attack and resulting data breach within a reasonable time, even though the risk of a data breach or theft was highly likely, especially given Defendants had been on notice for almost a year of the potential for a Hive ransomware attack on its systems. The business acts and practices by Defendants for failure to keep confidential medical, demographic or personal data protected, encrypted and without sufficient security to be breached by an adverse third party did not meet all applicable standards of care and vigilance. Tens if not hundreds of thousands of individuals are now prime targets for fraud, extortion, or access to other completely private information that would never have been provided to Defendants if the patients or consumers knew how negligent or reckless Defendants would be in not protecting such deeply personal medical and financial information private.

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

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

133. Plaintiff and Class members have no other adequate remedy of law in that absent injunctive relief from the Court Defendants are likely to not fully redress the issues raised by their illegal and unfair business practices. Defendants have not announced any specific changes to their data security infrastructure, processes or procedures to fix the vulnerabilities in the electronic information security systems and/or security practices that permitted the Hive ransomware attack and resulting data breach to occur and go undetected, and thereby prevent further attacks, nor have they provided prompt notice of the circumstances surrounding this breach as required by law.

134. Pursuant to Business & Professions Code section 17203, Plaintiff seeks an order of this Court both for himself, members of the Class and for the benefit of the public for injunctive relief in the form of requiring Defendants to correct their illegal conduct, to prevent Defendants from repeating the illegal and wrongful practices as alleged above and protect and preserve confidentiality of Medical Information in Defendants' possession that has been accessed, downloaded, exfiltrated, stolen, and viewed by at least one unauthorized third party because of Defendants' illegal and wrongful practices set forth above. Pursuant to Business & Professions Code section 17203, Plaintiff also seeks an order of this Court for equitable and/or injunctive relief in the form of prohibiting Defendants from continuing to refuse publicly issuing comprehensive direct and corrective notices.

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

FIFTH CAUSE OF ACTION

Declaratory Relief

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

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

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

139. Plaintiff and the Class members have no other adequate remedy of law in that absent declaratory relief from the Court, Defendants are likely to not fully remedy the underlying wrong.

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

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

PRAYER FOR RELIEF

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

A. Finding that this action satisfies the prerequisites for maintenance as a class action under California Code of Civil Procedure Section 382 and certifying the Class defined herein;

B. Designating Plaintiff as representative of the Class and his counsel as Class counsel;

C. Declaring Defendants' conduct in violation of the laws set forth above, including California Civil Code sections 56.10(a), 56.101, 1798.21, 1798.29, Business and Professions Code § 17200 *et seq.*, and Article I, § 1 of the California Constitution.

D. An order:

1. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

2. prohibiting Defendants from refusing to send all affected persons data breach notices regarding the ransomware attack and data theft at issue herein in the form and timing required by law, and publicly issue comprehensive corrective notices to Plaintiff, Class members and the public;

3. prohibiting Defendants from failing to protect, including through encryption, all data collected through the course of their business operations in accordance with all applicable regulations, industry standards, and federal and state laws;

4. prohibiting Defendants from refusing to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Medical Information, PII and PHI of Plaintiff and the Class members;

5. prohibiting Defendants from refusing to engage independent third-party security auditors/penetration testers as well as internal security personnel to run automated security monitoring, database scanning and security checks and conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

6. prohibiting Defendants from refusing to audit, test, and train security personnel regarding any new or modified procedures;

7. requiring Defendants to segment data by, among other things, creating firewalls

and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

8. prohibiting Defendants from refusing to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class members and infiltration of Defendants' computer system by phishing processes by using such steps such as multi-factor authentication;

9. prohibiting Defendants from refusing to routinely and continually conduct internal training and education, and inform internal security personnel how to immediately identify and contain a ransomware attack or data breach when it occurs and what to do in response to a breach; and,

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

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

F. Awarding Plaintiff's costs;

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

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

JURY DEMANDED

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

Dated: May 5, 2022

Respectfully submitted,

WHATLEY KALLAS, LLP

Alan M. Mansfield, SBN: 125998
16870 W. Bernardo Drive
Suite 400
San Diego, CA 92127
Phone: (619) 308-5034
Fax: (888) 341-5048
Email: amansfield@whatleykallas.com

WHATLEY KALLAS, LLP
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
152 W. 57th Street, 41st Floor
New York, NY 10019
Tel: (212) 447-7060
Fax: (800) 922-4851

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

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

DOYLE APC
William J. Doyle, SBN: 188069
550 West B Street
4th Floor
San Diego, CA 92101
Phone: (619) 736-0000
Fax: (619) 736-1111
Email: bill@doyleapc.com

Attorneys for Plaintiff