

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

Attorneys for Plaintiff

[Additional Counsel on Signature Page]

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

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

Plaintiff,

v.

PARKER-HANNIFIN CORPORATION, and
DOES 1 through 10, inclusive,

Defendants.

Case No.

**CLASS ACTION COMPLAINT FOR
VIOLATIONS OF:**

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

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

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

8 SUMMARY OF THE ACTION

9 1. Plaintiff brings this class action lawsuit his own behalf, and on behalf of a class of
10 similarly situated individuals defined below and for the benefit of the general public, against Defendants
11 arising from the failure by PARKER-HANNIFIN to adequately secure the Personal Information and/or
12 Medical Information (defined below) of Plaintiff and all others similarly situated who are current
13 residents and citizens of California.

14 2. As detailed more fully below, in March 2022 PARKER-HANNIFIN was subject to a
15 ransomware attack and accompanying data breach and theft by the Conti ransomware group (“Conti”).
16 On or about March 11, 2022, Conti gained access to Defendant PARKER-HANNIFIN’s computer
17 network, deployed malware that encrypted data in PARKER-HANNIFIN’s servers, and acquired over
18 400 gigabytes of employees’ personal information stored on Defendant PARKER-HANNIFIN’s
19 computer network servers (the “Data Breach”). It appears PARKER-HANNIFIN did not make a
20 ransomware payment, as now all of this employee data is available on the dark web. This impacted
21 Plaintiff and other similarly situated individuals who either are or were employed by PARKER-
22 HANNIFIN or are or were enrolled in PARKER-HANNIFIN’s Group Health Plan or a health plan
23 sponsored by an entity acquired by PARKER-HANNIFIN.

24 3. PARKER-HANNIFIN negligently created, maintained, preserved, and stored on its
25 computer systems Plaintiff’s and Class members’ personally individually identifiable Personal
26

27 ¹ Due to the sensitive nature of this action and the fact his information appears to be available on the
28 dark web, Plaintiff has elected to file under a pseudonym. (*See, e.g., Doe v. Kaweah Delta Hosp.*, 2010
U.S. Dist. LEXIS 135808 (E.D. Cal., Dec. 22, 2010); *Does I thru XXIII v. Advanced Textile Corp.* 214
F.3d 1058, 1067 (9th Cir. 2000).

1 Information and/or Medical Information. The personal information that may have been accessed and
2 taken includes PARKER-HANNIFIN and its subsidiaries employees' full names, Social Security
3 numbers, dates of birth, addresses, driver's license numbers, U.S. passport numbers, bank account and
4 routing numbers, online usernames and passwords ("Personal Information"). PARKER-HANNIFIN
5 failed to implement and maintain reasonable security procedures and practices appropriate to the nature
6 of the information at issue in order to protect Plaintiff's and others' personal information, which would
7 include Personal Information and Medical Information. Defendants' actions resulted in this information
8 being improperly accessed and copied by unauthorized third parties.

9 4. Defendants either knew, or reasonably should have known, the importance of
10 safeguarding the Medical Information and Personal Information entrusted to them and of the foreseeable
11 consequences if their computer network was breached. Defendants failed, however, to take adequate
12 measures to prevent the Conti ransomware attack. Defendants were on notice that they should have and
13 could have prevented this attack by properly securing and encrypting the information of Plaintiff and the
14 Class members and taking the steps outlined above to prevent infiltration by methods such as phishing
15 by, for example, using multi-factor authentication methods. Defendants could also have destroyed data
16 of former employees and their dependents that was no longer useful, especially outdated data for
17 individuals who either never worked for PARKER-HANNIFIN or left their employ years ago that for
18 some reason was retained on its computer network.

19 5. As a result, the Personal Information and Medical Information of a reported 119,513
20 individuals was compromised through disclosure to unknown and unauthorized third parties. PARKER-
21 HANNIFIN thus disclosed and/or permitted the disclosure of these persons' Medical Information and
22 Personal Information to unauthorized persons. An unknown but likely significant number of such
23 persons are residents and citizens of California and thus entitled to the unique statutory remedies available
24 under California law.

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

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

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

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

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

18 9. “Medical Information”, for purposes of this Complaint, includes health plan enrollment
19 information, health insurance plan ID numbers, and dates of coverage, and for a small subset of
20 individuals, the following sensitive information that may also have been accessed and acquired: dates of
21 medical coverage, dates of medical services, provider names, claims information and medical and clinical
22 treatment information. This term also refers to the above definition, and encompasses both Personal
23 Health Information (“PHI”), and Personally Identifiable Information (“PII”), including Social Security
24 numbers associated with individual health records within PARKER-HANNIFIN’s computer systems.

25 10. Since Medical Information encompasses such personal and revealing information, it is
26 highly valued as a gateway to medical identity theft⁵ and more general identity theft.⁶ Medical
27 Information has been found to command up to \$1,000 per individual record on the dark web.⁷ Thus,

28 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).

1 organizations such as Defendants, who are entrusted with this most sensitive and valuable data, have a
2 non-delegable duty to take particularly special care to maintain up-to-date information security practices
3 and keep apprised of industry-related threats as they arise. The threat from the Conti group of a
4 ransomware attack was reasonably foreseeable to Defendants, as companies had been warned for almost
5 a year of the potential for such an attack on their computer systems.

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

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

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

26 The Legislature hereby finds and declares that persons receiving health care services have
27 a right to expect that the confidentiality of individual identifiable Medical Information
28 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.

1 14. Consistent with that statutory purpose, the CMIA provides that “a provider of health care,
2 health care service plan, or contractor shall not disclose Medical Information regarding a patient of the
3 provider of health care or an enrollee or subscriber of a health care service plan without first obtaining
4 an authorization [. . .].” (Cal. Civ. Code § 56.10(a).) Defendants’ actions permitted the disclosure of the
5 Medical Information at issue here to unauthorized third parties.

6 15. Additionally, Civ. Code Section 56.101(a) states, in relevant part, that every health care
7 provider or health care service plan that creates, maintains, preserves, or stores Medical Information shall
8 do so in a manner that preserves its confidentiality. Defendants’ actions establish that they did not
9 maintain the Medical Information at issue in a manner that preserved its confidentiality, as it was able to
10 be improperly accessed and copied by unauthorized third parties, including the Conti group. PARKER-
11 HANNIFIN’s failure to create, maintain, preserve, and store Medical Information in a manner that
12 preserved the confidentiality of the information contained therein resulted in the illegal access,
13 authorization, exfiltration, disclosure, negligent release and/or theft of over 400 gigabytes of data related
14 to PARKER-HANNIFIN current and former employees, their dependents and members of PARKER-
15 HANNIFIN’s group health plans (including health plans sponsored by an entity acquired by PARKER-
16 HANNIFIN), which necessarily included PII, PHI and Medical Information.

17 16. Defendants had obligations under California Civil Code Sections 56.20(a) and (c) to
18 ensure, as an employer, that (1) if they received Medical Information about their employees, that they
19 would establish appropriate procedures to ensure the confidentiality and protection from unauthorized
20 use and disclosure of that information; and (2) that they would not disclose or knowingly permit their
21 employees or agents to disclose Medical Information about their employees without a signed
22 authorization.

23 17. Defendants’ violations of California Civil Code §§ 56.20(a) and (c) subject them to the
24 remedies afforded under California Civil Code §§ 56.35 and 56.36(b).

25 18. The remedies provided for under California Civil Code Section 56.35 allow private
26 litigants whose Medical Information has been used or disclosed in violation of California Civil Code §
27 56.20 or/and who have sustained economic loss to recover compensatory damages, punitive damages not
28 to exceed \$3,000 per class member, attorney fees not to exceed \$1,000 per class member and the costs

1 of litigation. However, these are only partial remedies as they do not resolve the underlying issue,
2 protecting Plaintiff and Class members from misuse of their data or further attacks, including, but not
3 limited to, fraudulent use of their financial information, identity theft, use of their medical information
4 to fraudulently secure and pay for medical services, use of Social Security numbers to file false tax
5 returns, steal tax refunds or gain employment under an assumed identity, and opening credit under false
6 credentials. Nor do these monetary remedies help Plaintiff and Class members monitor or remove this
7 data to prevent further abuses on the dark web.

8 19. Defendants disregarded the rights of Plaintiff and members of the Class by negligently
9 failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and the Class
10 members' Personal Information and Medical Information was safeguarded, failing to take available steps
11 to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate
12 protocols, policies and procedures regarding data access and encryption, even for internal use, as well as
13 appropriate procedures that would prevent such intrusions through methods such as phishing, like multi-
14 factor authentication..

15 20. Defendants' actions additionally violated the California Consumer Privacy Act
16 ("CCPA"), California Code §§ 1798.100 *et seq.*, in that they failed to keep the nonencrypted and
17 nonredacted personal information of Plaintiff and all similarly situated persons from unauthorized access
18 and exfiltration, theft or disclosure as a result of Defendants' violation of their duty to implement and
19 maintain reasonable security procedures and practices appropriate to the nature of the information to
20 protect that Personal Information. The personal information at issue relevant to this violation includes,
21 but is not limited to: Social Security numbers, driver's license numbers, U.S. passport numbers, medical
22 information, and health insurance information.

23 21. Based on Defendants' violation of the CCPA as described herein, Plaintiff and all
24 similarly situated persons therefore are entitled to bring a private action pursuant to California Civil Code
25 Section 1798.150(a). PARKER-HANNIFIN's failure to adequately protect the nonpublic Personal
26 Information and Medical Information in their possession has likely caused, and will continue to cause,
27 substantial harm and injuries to Plaintiff and Class members. Plaintiff and all other similarly situated
28 individuals face a long-term battle against identity theft if their full names, Social Security numbers, dates

1 of birth, addresses, drivers' license and passport numbers and other sensitive personal and financial
2 information were contained in this unauthorized access and exfiltration. Plaintiff and the Class members
3 have a continuing interest in ensuring that their information is and remains safe.

4 22. As shown by PARKER-HANNIFIN's total shutdown of certain systems in response to
5 this cyber event, Defendants' unlawful conduct presents an imminent and impending continuing risk for
6 Plaintiff and Class members, particularly where PARKER-HANNIFIN refuses to disclose any of the
7 details about the ransomware attack – including that this data is now accessible on the dark web. As a
8 result of Defendants' conduct and the ensuing Data Breach, Plaintiff and the members of the proposed
9 Class have suffered damages, and are additionally at imminent risk of future harm, including identity
10 theft and fraud.

11 Accordingly, Plaintiff brings this action on behalf of himself and Class of all others similarly situated
12 and for the benefit of the general public, to seek redress for Defendants' unlawful conduct. Plaintiff and
13 the Class are thus entitled to injunctive relief, legal equitable relief, damages, costs and expenses of
14 litigation, and attorneys' fees.

15 **JURISDICTION AND VENUE**

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

20 24. Venue is appropriate in this District under 28 U.S.C. § 1391 because a substantial part of
21 the events or omissions giving rise to the claim occurred in this District, and Plaintiff and other class
22 members reside in this District.

23 **PARTIES**

24 25. On personal knowledge, Plaintiff John Doe is a citizen and current resident of the State of
25 California. Plaintiff, in the course of his employment with PARKER-HANNIFIN or a subsidiary thereof,
26 was required to provide sensitive Personal Information, including his Social Security number, driver's
27 license, passport number and banking information. Plaintiff was also a former enrollee of PARKER-
28 HANNIFIN's Group Health Plan, and in connection therewith also provided Defendants with

1 individually identifiable information and Medical Information, as defined by Civil Code section 56.05(i).
2 While Defendant has yet to provide the particulars, it is likely some amount of Plaintiff's Medical
3 Information was created, maintained, preserved, and stored onto Defendant's computer network. Such
4 Medical Information included or contained an element of personal identifying information sufficient to
5 allow identification of the individual, such as name, date of birth, address, and Social Security number,
6 and additionally likely also contained medical record number, insurance provider, electronic mail
7 address, telephone number, or other information that, alone or in combination with other publicly
8 available information, reveals Plaintiff's identity. Given the highly sensitive nature of the information
9 stolen in the Data Breach, Plaintiff remains at a substantial and imminent risk of future harm, including
10 identity theft and theft from his bank accounts. Plaintiff has expended and will be required to expend
11 time and effort monitoring his financial accounts and credit reports. Through the exfiltration of such
12 data, he has been injured in fact and lost money or property as a result of Defendants' misconduct in
13 having his Personal Information and/or Medical Information likely disclosed to and stolen by third parties
14 without his authorization, and the confidentiality and integrity of his Medical Information breached, lost,
15 not preserved, and not protected. Plaintiff has also experienced fear, anxiety, and worry caused by the
16 unauthorized disclosure of Personal Information and Medical Information by PARKER-HANNIFIN
17 since he became aware of it and received a letter from PARKER-HANNIFIN offering limited credit
18 monitoring services.

19 26. Defendant Parker-Hannifin Corporation is an Ohio Corporation, with offices located
20 around the United States, including in this District.

21 27. The true names, roles, and capacities in terms of their involvement in the wrongdoing at
22 issue, whether individual, corporate, associate, or otherwise, of Defendants named as DOES 1 through
23 10, inclusive, are currently unknown to Plaintiff and, therefore, are named as Defendants under fictitious
24 names. Plaintiff will identify these Defendants' true identities and their involvement in the wrongdoing
25 at issue if and when they become known.

26 28. Defendants' conduct described herein, including reviewing, approving, or ratifying the
27 conduct at issue, was undertaken either directly by PARKER-HANNIFIN or as an agent, servant,
28 contractor, or employee of PARKER-HANNIFIN, and/or was performed within the course and scope of

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

3 **FACTUAL ALLEGATIONS**

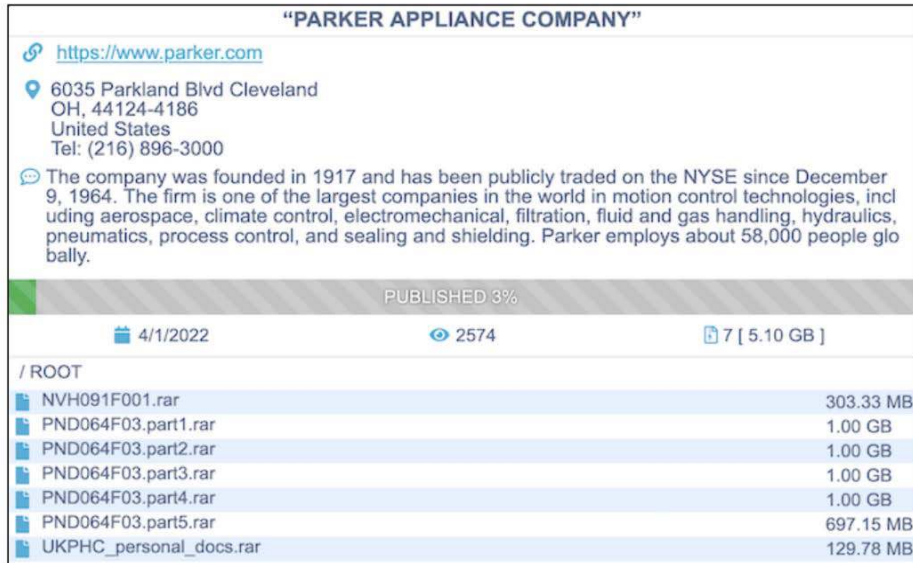
4 **A. THE NATURE OF THE RANSOMWARE ATTACK.**

5 29. On or about May 12, 2022, PARKER-HANNIFIN reported a data breach affecting almost
6 120,000 current and former employees, their dependents, and others, both of PARKER-HANNIFIN and
7 numerous of its subsidiaries.

8 30. In addition, current or former enrollees of PARKER-HANNIFIN's Group Health Plan (or
9 a health plan sponsored by an entity acquired by PARKER-HANNIFIN), may also have been subject to
10 unauthorized access and theft.

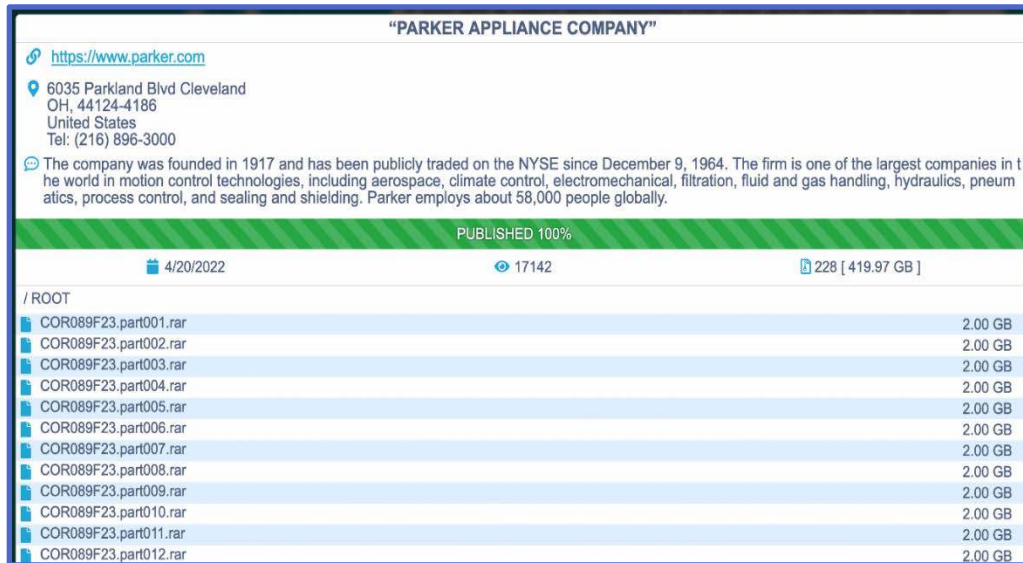
11 31. PARKER-HANNIFIN's public statement about this data breach and ransomware attack
12 was first disclosed in a Form 8-K filed with the Securities and Exchange Commission on or about April
13 5, 2022, which stated that "a third party gained unauthorized access to the Company's systems" from
14 March 11-14, 2022. PARKER-HANNIFIN's filing also stated that "the Company believes some data
15 was accessed and taken and may include personal information of Company team members." PARKER-
16 HANNIFIN did not begin notifying affected individuals until on or about May 13, 2022, two months
17 after the Data Breach.

18 32. While not included in PARKER-HANNIFIN's public statements about this incident,
19 *Security Week* reports that Parker's attack was perpetrated by the Conti ransomware group. On or about
20 April 1, 2022 the Conti group published 5 GB of the stolen files on the dark web, which purportedly was
21 only 3% of the data taken.



screenshot of the Conti data leak page published by Security Week (<https://www.securityweek.com/ransomware-gang-leaks-files-stolen-industrial-giant-parker-hannifin>)

Typically, this sort of publication is initially done to prove the personal data has been successfully stolen.



(screenshot of the Conti data leak page for PARKER-HANNIFIN as of May 19, 2022)

33. On or about April 20, 2022, Conti announced through its data leak page that 100% of the data taken from PARKER-HANNIFIN has been published. The size of the data purportedly released to the dark web for open access is 419.97 GB. It further appears that this data leak page has been publicly viewed and accessed over 17,000 times.

34. According to a report recently filed with the U.S. Department of Health and Human

1 Services, PARKER-HANNIFIN has reported that 119,513 people are impacted by the Data Breach.

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

4 36. The only clue PARKER-HANNIFIN provided that it had been subject to a ransomware
5 attack and had Personal Information and Medical Information of over 100,000 employees stolen from its
6 servers was that it told individuals, in a notice sent on or about May 12, 2022, that an unauthorized person
7 had gained access to its IT servers. Despite its duties and obligations under California law to promptly
8 provide notice to consumers of such material facts so that they could take appropriate action, PARKER-
9 HANNIFIN did not inform members for two months that an unauthorized party accessed and may have
10 acquired certain files on PARKER-HANNIFIN's IT systems that contain information pertaining to a
11 significant number of current and former PARKER-HANNIFIN employees, their dependents, and other
12 individuals affiliated with the company or its subsidiaries. To date, PARKER-HANNIFIN has never
13 disclosed that it was the subject of a ransomware attack, that its systems had been encrypted by the Conti
14 ransomware group, whether or not it paid the ransom, and that all of this Medical Information, Personal
15 Information and personal financial information had been stolen and was disclosed on the internet.

16 **B. PARKER-HANNIFIN WAS ON NOTICE OF THE POTENTIAL FOR THIS
17 ATTACK.**

18 37. PARKER-HANNIFIN has been on notice for almost a year of the potential for a Conti
19 ransomware attack on its systems but did not take sufficient steps to prevent it.

20 38. PARKER-HANNIFIN's negligence in safeguarding the Medical Information, Personal
21 Information and personal financial information of Plaintiff and the Class members was exacerbated by
22 the repeated warnings and alerts directed to U.S. companies, warning that they should protect and secure
23 sensitive data, especially in light of the substantial increase in cyberattacks by the Conti ransomware
24 group.

25 39. The FBI has been warning companies such as PARKER-HANNIFIN about the threat
26 posed by the Conti ransomware group, and to be on the lookout for attacks from this group, for a year. It
27 issued a [Flash Alert](#) about Conti ransomware attacks in May, 2021, and a [Joint Cybersecurity Advisory](#)
28 on September 22, 2021, which was updated most recently on March 9, 2022 – *two days before this attack*

1 *took place*. The Advisory was disseminated with details about what red flags indicate a business has been
2 compromised by Conti ransomware, and how attacks can be avoided.

3 40. Specifically, as early as May 20, 2021, the FBI issued a Flash Alert that detailed the threat
4 posed by the Conti group. It highlighted that “among the more than 400 organizations worldwide
5 victimized by Conti, over 290 of which are located in the U.S. Like most ransomware variants, Conti
6 typically steals victims’ files and encrypts the servers and workstations in an effort to force a ransom
7 payment from the victim. The ransom letter instructs victims to contact the actors through an online portal
8 to complete the transaction. If the ransom is not paid, the stolen data is sold or published to a public site
9 controlled by the Conti actors.”⁸

10 41. In the initial FBI Flash Alert, the FBI included a lengthy list of recommended mitigations
11 businesses should take in order to avoid or minimize the effects of a Conti attack, including:

- 12 • Regularly back up data, air gap, and password protect backup copies offline. Ensure
13 copies of critical data are not accessible for modification or deletion from the system
14 where the data resides.
- 15 • Implement network segmentation.
- 16 • Implement a recovery plan to maintain and retain multiple copies of sensitive or
17 proprietary data and servers in a physically separate, segmented, secure location (i.e., hard
18 drive, storage device, the cloud).
- 19 • Install updates/patch operating systems, software, and firmware as soon as they are
20 released.
- 21 • Use multifactor authentication where possible.
- 22 • Use strong passwords and regularly change passwords to network systems and accounts,
23 implementing the shortest acceptable timeframe for password changes. Avoid reusing
24 passwords for multiple accounts.
- 25 • Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- 26 • Require administrator credentials to install software.

27 _____
28 ⁸ FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks (May 20,
2021); <https://www.ic3.gov/Media/News/2021/210521.pdf>.

- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Consider adding an email banner to messages coming from outside your organizations.
- Disable hyperlinks in received emails.
- Focus on cyber security awareness and training.
- Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e., ransomware and phishing scams).⁹

42. On September 22, 2021, in continuing efforts to alert businesses and their employees about the growing Conti threat, the FBI and NSA sent out warning about the Conti group over Twitter,



⁹ *Id.*

1 with a call to take “immediate action.” (tweet from [@NSACyber](#) last accessed May 19, 2022 below).

2 43. On that same day, September 22, 2021, the U.S. Cybersecurity & Infrastructure Security
3 Agency (“CISA”), in conjunction with the FBI and NSA published a Joint Cybersecurity Advisory on
4 Conti Ransomware.¹⁰

5 44. In that Joint Cybersecurity Advisory, CISA provided businesses with a lengthy listing of
6 technical details that explained how the group was gaining initial access to business IT networks,
7 indicators that would let businesses know they had been compromised, techniques used by Conti to
8 compromise IT systems, and yet again, another list of recommended mitigations to reduce the risk of
9 compromise from Conti ransomware attacks, with additional mitigations not previously included in the
10 FBI Flash Alert.¹¹ The 10-page technical treatise also provided references to other helpful materials for
11 businesses with links, and an offer for “Free Cyber Hygiene Services” offered by CISA to help
12 organizations “assess, identify, and reduce their exposure to threats, including ransomware.”¹² The
13 increase in such attacks, and the attendant risk of future attacks, was widely known within PARKER-
14 HANNIFIN’s business community. Due to the high-profile nature of these breaches and attacks,
15 Defendants either were or should have been on heightened notice and aware of such attacks and, therefore,
16 should have been on notice of their duty to be proactive in guarding against being subject to such attacks
17 and adequately performed their duty of preparing for and immediately identifying such an attack.

18 45. Yet despite the prevalence of public announcements of these data breach and data security
19 compromises and despite numerous attempts on the part of the federal government to inform government
20 contractor companies like PARKER-HANNIFIN of the threat posed by ransomware attacks in general
21 and Conti in particular, and despite having almost a year from their attack to prepare and prevent such
22 an attack, PARKER-HANNIFIN was negligent and did not adequately prepare for this wholly
23 foreseeable event, allowing extremely sensitive data to be accessed, viewed and stolen by the Conti
24 ransomware group. Defendants thus breached their duty to take appropriate steps to protect Plaintiff’s
25

26 ¹⁰ See, Joint Cybersecurity Advisory: Conti Ransomware (9/22/21);
27 [https://www.cisa.gov/uscrt/sites/default/files/publications/AA21-265A-
Conti_Ransomware_TLP_WHITE.pdf](https://www.cisa.gov/uscrt/sites/default/files/publications/AA21-265A-Conti_Ransomware_TLP_WHITE.pdf) (last accessed May 24, 2022).

28 ¹¹ *Id.*

¹² *Id.* page, 9.

1 and Class members' Personal Information and/or Medical Information from being compromised and
2 have failed to adequately notify such persons that such a ransomware attack has taken place.

3 46. Unfortunately for Plaintiff and other similarly situated individuals, their Personal
4 Information and Medical Information was not secured in the manner required under California law that
5 would have prevented this Conti attack. What's worse, despite Defendants' obligations under the law to
6 promptly notify affected individuals so they can take appropriate action, Defendants failed to promptly
7 provide such notice in the most expedient time possible and without unreasonable delay, failed to include
8 in the data breach notice a sufficient description of the data breach incident to comply with Civil Code
9 Section 1798.29(d)(2)(E), and any other relevant laws, and failed to provide in the Data Breach notice
10 the information needed by Plaintiff and other similarly situated individuals to enable them react
11 appropriately to the breach, including taking whatever mitigation measures are necessary.

12 47. As a result, this unauthorized access, disclosure, and exfiltration remains unremedied.
13 Defendants have failed to provide notice to affected consumers in the most expedient time possible and
14 without unreasonable delay, as required under California law.

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

17 48. Defendants are required by the CCPA, the CMIA and various other laws and regulations
18 to protect Plaintiff's and Class members' Personal Information and Medical Information and to handle
19 notification of any breach in accordance with applicable breach notification statutes. Failing to do so
20 results in acts of negligence *per se* by Defendants. These duties are established in numerous California
21 statutes, including California Civil Code Sections 56.101, 1798.150(a) and 1798.82.

22 49. In addition, as federal government contractors, Defendants made representations that they
23 would comply with numerous cybersecurity requirements applicable to the protection of data on their
24 computer systems, including but not limited to Federal Acquisition Regulation 52.204-21 and Defense
25 Federal Acquisition Regulation Supplement 252.204-7012, which impose physical and cybersecurity
26 obligations on contractor systems that process government information.

27 50. In addition, to the extent that PHI was affected by the Data Breach, as Defendants may be
28 entities covered by the Health Insurance Portability and Accountability Act ("HIPAA") (45 C.F.R. §

1 160.102) they are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part
2 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health
3 Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health
4 Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C, which establish national security
5 standards and duties for Defendants’ protection of Medical Information maintained by them in electronic
6 form.

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

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

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

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

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

28 (a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendants

1 create, receive, maintain, and transmit, in violation of 45 C.F.R. section
2 164.306(a)(1);

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

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

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

12 (e) Failing to protect against any reasonably-anticipated threats or hazards to the
13 security or integrity of electronic PHI, in violation of 45 C.F.R. section
14 164.306(a)(2);

15 (f) Failing to protect against any reasonably anticipated uses or disclosures of
16 electronic PHI that are not permitted under the privacy rules regarding individually
17 identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);

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

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

23 (i) Failing to effectively train all members of its workforce (including independent
24 contractors) on the policies and procedures with respect to PHI as necessary and
25 appropriate for the members of its workforce to carry out their functions and to
26 maintain security of PHI, in violation of 45 C.F.R. sections 164.530(b) and
27 164.308(a)(5); and

28 (j) Failing to design, implement, and enforce policies and procedures establishing

1 physical and administrative safeguards to reasonably safeguard PHI in compliance
2 with 45 C.F.R. section 164.530(c).

3 56. Defendants also violated the duties applicable to them under the Federal Trade
4 Commission Act (15 U.S.C. § 45 *et seq.*) from engaging in “unfair or deceptive acts or practices in or
5 affecting commerce.” The FTC pursuant to that Act has concluded that a company’s failure to maintain
6 reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair
7 practice” in violation of the FTC Act.¹³

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

28 ¹³ See, e.g., *FTC v. Wyndham Worldwide Corp.*, (3d Cir. 2015) 799 F.3d 236.

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

11 59. As a direct and proximate result of Defendants' actions, inactions, omissions, breaches of
12 duties and want of ordinary care that directly and proximately caused or resulted in the ransomware attack
13 and the resulting data breach, Plaintiff and Class members have suffered and will continue to suffer
14 damages and other injury and harm not fully compensable by the payment of damages in the form of,
15 *inter alia*, (a) present, imminent, immediate and continuing increased risk of identity theft, identity fraud
16 and medical fraud -- risks justifying expenditures for protective and remedial services for which they are
17 entitled to compensation, (b) invasion of privacy, (c) breach of the confidentiality of their Personal
18 Information and Medical Information, (d) deprivation of the value of their Personal Information and
19 Medical Information, for which there is a well-established national and international market, as well as
20 statutory damages to which they are entitled even without proof of access or actual damages; (e) the
21 financial and temporal cost of monitoring their credit reports, (f) increased risk of future harm, and/or (g)
22 fear, anxiety, and worry caused by the unauthorized release of their Personal Information and Medical
23 Information, all resulting in a loss of money or property related to Defendants' misconduct.

1 **D. THE VALUE OF PERSONAL INFORMATION AND MEDICAL**
2 **INFORMATION SHOWS THAT PLAINTIFF AND OTHERS LOST VALUABLE**
3 **MONEY OR PROPERTY AS A RESULT OF THIS ATTACK AND DO NOT**
4 **HAVE AN ADEQUATE REMEDY AT LAW.**

5 60. It is well known that Personal Information and Medical Information is a valuable
6 commodity¹⁴ and the frequent target of hackers, such that Plaintiff and Class members would lose money
7 or property if their data was permitted to be improperly accessed or stolen and that they would not have
8 an adequate remedy at law simply by receiving payment for damages and limited credit monitoring.

9 61. The unauthorized disclosure of Social Security numbers can be particularly damaging
10 because Social Security numbers cannot easily be replaced. In order to obtain a new number, a person
11 must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, under
12 current rules, no new number can be obtained until damage has been done. Furthermore, as the Social
13 Security Administration warns: “A new number probably will not solve all your problems. This is
14 because other governmental agencies (such as the Internal Revenue Service and state motor vehicle
15 agencies) and private businesses (such as banks and credit reporting companies) likely will have records
16 under your old number. Also, because credit reporting companies use the number, along with other
17 Personal Information, to identify your credit record, using a new number will not guarantee you a fresh
18 start. This is especially true if your other Personal Information, such as your name and address, remains
19 the same. If you receive a new Social Security Number, you will not be able to use the old number
20 anymore.” Social Security Administration, Identity Theft and Your Social Security Number (June 2017),
21 available at <http://www.ssa.gov/pubs/10064.html> (last visited Nov. 22, 2019).

22 62. For some victims of identity theft, a new Social Security number actually creates new
23 problems. If the old credit card information is not associated with the new number, the absence of any
24 credit history under the new number may make it more difficult for you to get credit.

25 63. According to the Attorney General of the United States, Social Security numbers “can be
26 an identity thief’s most valuable piece of consumer information.” Fact Sheet: The Work of the President’s
27 Identity Theft Task Force, DOJ 06-636, 2006 WL 2679771 (Sep. 19, 2006). Indeed,: “The ubiquity of

28 ¹⁴ 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).

1 the SSN as an identifier makes it a primary target for both hackers and identity thieves. . . . When data
2 breaches expose SSNs, thieves can use these numbers—usually combined with other pieces of data—to
3 impersonate individuals and apply for loans, housing, utilities, or government benefits. Additionally, this
4 information may be sold on the black market to other hackers.” Daniel J. Marcus, *The Data Breach*
5 *Dilemma: Proactive Solutions for Protecting Consumers’ Personal Information*, 68 *Duke L.J.* 555, 564–
6 65 (2018).

7 64. Defendants either were or should have been aware that the Personal Information, Medical
8 Information, PII and PHI they collected and retained is highly sensitive and of significant value to those
9 who would use it for wrongful purposes months if not years after the breach took place. As the FTC has
10 reported, identity thieves can use this information to commit an array of crimes including identify theft,
11 medical and financial fraud.¹⁵ Medical identity theft is one of the most common, most expensive, and
12 most difficult-to-prevent forms of identity theft.

13 65. Indeed, a robust cyber black market exists in which criminals post stolen Medical
14 Information, PII and PHI on multiple underground Internet websites, commonly referred to as the dark
15 web, to create fake insurance claims, purchase and resell medical equipment, or access prescriptions for
16 illegal use or resale. According to a 2017 Javelin strategy and research presentation, fraudulent activities
17 based on data stolen in data breaches that is between two and six years old had increased by nearly 400%
18 over the previous four years.¹⁶ Thus, an offer of credit monitoring service that is only for two years is not
19 an adequate remedy or offer, even if it conducts dark web scanning (which is unclear here).

20 66. According to Experian, one of the three major credit bureaus, medical records can be
21 worth up to \$1,000 per person on the dark web, depending upon completeness.¹⁷ PII and PHI can be sold
22 at a price ranging from approximately \$20 to \$300.¹⁸

23 67. In this case, all evidence indicates that Plaintiff and Class Members’ Personal Information
24 and Medical Information were left unprotected, to be freely accessed on the dark web by the Conti group

25 ¹⁵ Federal Trade Commission, *What To Know About Identity Theft*,
26 <https://consumer.ftc.gov/articles/what-know-about-identity-theft> (last accessed 5/3/22).

27 ¹⁶ *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-](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/)
28 [selling-for-on-the-dark-web/](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/) (last accessed 5/23/22).

¹⁷ *Id.*

¹⁸ <https://www.privacyaffairs.com/dark-web-price-index-2021/>

1 after exfiltration. Thus, this highly valuable data was left to be pilfered by criminals or reviewed by
2 anyone with an Internet connection – and has been accessed at least 17,000 times already.

3 68. Medical identify theft can also result in inaccuracies in medical records and costly false
4 claims. It can also have life-threatening consequences since if a victim’s health information is mixed with
5 other records, it can lead to misdiagnosis or mistreatment. “Medical identity theft is a growing and
6 dangerous crime that leaves its victims with little to no recourse for recovery,” reported Pam Dixon,
7 executive director of World Privacy Forum. “Victims often experience financial repercussions and worse
8 yet, they frequently discover erroneous information has been added to their personal medical files due to
9 the thief’s activities.”¹⁹

10 69. The Ponemon Institute found that medical identity theft can cost victims an average of
11 \$13,500 to resolve per incident, and that victims often have to pay off the imposter’s medical bills to
12 resolve the breach.²⁰

13 70. In another study by the Ponemon Institute in 2015, 31% of medical identity theft victims
14 lost their healthcare coverage as a result of the incident, while 29% had to pay to restore their health
15 coverage, and over half were unable to resolve the identity theft at all.²¹

16 71. Once Personal Information and Medical Information is stolen, particularly such as
17 membership identification numbers or Social Security numbers, fraudulent use of that information and
18 damage to victims may continue for years, as the fraudulent use of such data resulting from the attack
19 may not come to light for years. According to the U.S. Government Accountability Office (“GAO”),
20 which conducted a study regarding data breaches: “[L]aw enforcement officials told us that in some
21 cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further,
22 once stolen data have been sold or posted on the Web, fraudulent use of that information may continue
23

24 ¹⁹ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, (2/7/14),
25 <https://khn.org/news/rise-of-identity-theft/> (last accessed 5/3/22); *See also, Medical Identity Theft in*
the New Age of Virtual Healthcare, IDX (March 15, 2021), [https://www.idx.us/knowledge-](https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare)
[center/medical-identity-theft-in-the-new-age-of-virtual-healthcare](https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare) (last accessed 5/3/22).

26 ²⁰ Brian O’Connor, Healthcare Data Breach: What to Know About Them and What to Do After One,
27 Experian (June 14, 2018), [https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-](https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/)
[to-know-about-them-and-what-to-do-after-one/](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).

28 ²¹ 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).

1 for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot
2 necessarily rule out all future harm.”²²

3 72. The ramifications of Defendants’ failure to keep the Personal Information and Medical
4 Information in question secure from attack and then not advise affected persons of all the relevant facts
5 is thus not temporary but long lasting, as the fraudulent use of that information and damage to victims
6 may continue for years, and long after the expiration of any offered credit monitoring services. Criminals
7 often trade stolen medical information, PII and PHI on the “cyber black market” for years following a
8 breach. For example, it is believed that certain PHI/PII compromised in the 2017 Experian data breach
9 was being used three years later by identity thieves to apply for COVID-19-related benefits.²³ That is one
10 of the reasons providing prompt notice to consumers as expeditiously as possible is necessary, so they
11 can take actions to protect themselves. Yet Defendants are still refusing to even acknowledge that a
12 ransomware and resulting data breach took place, let alone provided comprehensive notice in the most
13 expedient time possible and without unreasonable delay, as required under California law.

14 73. For all these reasons, Plaintiff and Class members thus have no other adequate remedy at
15 law since the payment of actual and statutory damages will not adequately address these realities. Absent
16 injunctive relief from the Court Defendants are likely to not fully redress the issues raised by their illegal
17 and unfair business practices. Defendants have not announced any specific changes to their data security
18 infrastructure, processes, or procedures to fix the vulnerabilities in the electronic information security
19 systems and/or security practices that permitted the Conti ransomware attack and the Data Breach to
20 occur and go undetected, and thereby prevent further attacks, nor did they provide complete and prompt
21 notice of the circumstances surrounding this breach as required by law.

22 CLASS ALLEGATIONS

23 74. Plaintiff, on behalf of himself and all others similarly situated, brings this action pursuant
24

25 ²² *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full*
26 *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).

27 ²³ Janelle Stecklein, *Director: 64,000-plus fraudulent unemployment claims’ mitigated*, The Duncan
28 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)

1 to Fed R. Civ. Proc. 23. This action satisfies the numerosity, commonality, typicality, adequacy,
2 predominance, and superiority requirements for class certification.

3 75. The proposed class (“Class”) is defined as:

4 All current California residents who are present or former employees of PARKER-
5 HANNIFIN or one of its subsidiaries and whose information was accessed and released or
6 disclosed as a result of the Conti ransomware attack in or about March, 2022.

7 The Class also contains a sub-Class (“the Medical Information Sub-class”) that consists of
8 all persons who fall within the definition of the Class whose Medical Information was
9 accessed and released or disclosed as a result of the Conti ransomware attack in or about
10 March, 2022.

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

13 77. The members of the Class are sufficiently numerous such that joinder of all Class
14 members is impracticable. The proposed Class contains past or current PARKER-HANNIFIN or
15 subsidiary employees, certain of their dependents, and certain members of PARKER-HANNIFIN’s
16 group health plans or a health plan sponsored by an entity acquired by PARKER-HANNIFIN that,
17 according to a recent filing with the HHS Office of Civil Rights, consists of 119,513 individuals.

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

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

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

(c) Whether Defendants negligently created, maintained, preserved, stored, abandoned, or
disposed of Plaintiff’s and Class members’ Personal Information and Medical Information, and failed to

1 protect and preserve the integrity of the Personal Information and Medical Information found on
2 PARKER-HANNIFIN's computer systems;

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

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

9 (f) Whether Defendants have adequately addressed and fixed the vulnerabilities in their
10 computer system that permitted the ransomware attack and resulting data breach to occur;

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

15 (h) Whether Defendants violated California's CCPA, CMIA and the other laws cited herein;
16 and

17 (i) Whether Plaintiff and the Class are entitled to damages, equitable relief and/or injunctive
18 relief to redress the imminent and currently ongoing harm faced as a result of the Conti ransomware
19 attack and Defendants' failure to provide notice thereof, and the scope of such relief.

20 79. Plaintiff's claims are typical of the claims of other Class members. There is no unique
21 defense available to Defendants as Plaintiff, like all Class members, was a PARKER-HANNIFIN
22 employee, was enrolled in PARKER-HANNIFIN's health services plan and was apparently subjected to
23 the unauthorized disclosure of Personal Information and Medical Information as a result of Defendants'
24 conduct.

25 80. Plaintiff will fairly and adequately represent the interests of the Class members. Plaintiff
26 has retained counsel with substantial experience in prosecuting complex litigation and class actions,
27 including data breaches concerning the sensitive Personal Information and Medical Information of
28 individuals. Plaintiff and his counsel are committed to vigorously prosecuting the action on behalf of the

1 Class. Neither Plaintiff nor his counsel has any interest adverse to or that irreconcilably conflicts with
2 those of other Class members.

3 81. Absent a class action, most members of the Class would find the cost of litigating their
4 claims to be prohibitive and may have no effective and complete remedy. Class treatment of common
5 questions of law and fact is also superior to multiple individual actions or piecemeal litigation and results
6 in substantial benefits in that it conserves the resources of the courts and litigants and promotes
7 consistency and efficiency of adjudication. The conduct of this action as a class action presents few
8 management difficulties and protects the rights of each Class member. Plaintiff thus anticipates no
9 difficulty in the management of this case as a class action and providing notice to members of the Class.

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

13 CAUSES OF ACTION

14 FIRST CAUSE OF ACTION

15 **Violation of the California Consumer Privacy Act**

16 **Cal. Civ. Code § 1798.100 *et seq.***

17 83. Plaintiff incorporates the foregoing allegations as if fully set forth herein. This count is
18 brought on behalf of the Class and the Sub-Class. Plaintiff does not assert a claim for damages at this
19 time under this Cause of Action and does not incorporate by reference any allegations pertaining to
20 requests for damages.

21 84. The CCPA was enacted to protect consumers' sensitive information from collection and
22 use by businesses without appropriate notice and consent.

23 85. Through the above-detailed conduct, Defendant violated CCPA by subjecting the
24 nonencrypted and nonredacted Personal Information of Plaintiff and Class members to unauthorized
25 access, theft, or disclosure as a result of Defendant's violation of its duty to implement and maintain
26 reasonable security procedures and practices appropriate to the nature and protection of that information.
27 Cal. Civ. Code § 1798.150(a). In accordance with Cal. Civ. Code § 1798.150(b), Plaintiff's counsel has
28 sent a Notice of Violation to PARKER-HANNIFIN on behalf of Plaintiff and all other similarly situated

1 California residents. Plaintiff does not assert claims for damages at this time for his claim under the
2 CCPA, but reserves the right to do so if Defendants do not timely respond to and accept Plaintiff's claim
3 for damages, on behalf of both himself and all others similarly situated.

4 86. On behalf of Class members, Plaintiff seeks injunctive relief in the form of an order
5 enjoining Defendant from continuing to violate the CCPA. If Defendant fails to timely respond to
6 Plaintiff's notice letter or agree to rectify the violations detailed above, Plaintiff also will seek actual and
7 punitive damages, Plaintiff will also seek statutory damages of between \$100 and \$750 per Class
8 member, attorneys' fees and costs, and any other relief the Court deems proper as a result of Defendant's
9 CCPA violations.

10 **SECOND CAUSE OF ACTION**

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

12 **Cal. Civ. Code § 56 *et seq.***

13 87. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein.
14 The Cause of Action is brought on behalf of the Medical Information Sub-class.

15 88. PARKER-HANNIFIN is subject to the requirements of the CMIA as an employer under
16 Cal. Civ. Code Section 56.20(a) and as a corporation that receives Medical Information regarding a
17 patient under California Civil Code Section 56.10(e), which as noted above it admits to having received.

18 89. PARKER-HANNIFIN must not disclose or permit the disclosure of Medical Information
19 regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan
20 without first obtaining authorization, subject to certain exceptions found in Civil Code Section 56.10(b)
21 & (c) that do not apply here. (Cal. Civ. Code §§ 56.10(a) & (e).) Further, to the extent the PARKER-
22 HANNIFIN was an employer of Plaintiff and Class members, it is prohibited from using disclosing, or
23 knowingly permitting its employees or agents to use or disclose Medical Information that PARKER-
24 HANNIFIN possesses pertaining to its employees without the patient having first signed an authorization,
25 except under certain exceptions not relevant to this action. Additionally, to the extent the PARKER-
26 HANNIFIN was an employer to Plaintiff and Class members, it was also required to establish appropriate
27 procedures to ensure the confidentiality and protection from unauthorized use and disclosure of Medical
28 Information it has received, including, but not limited to instruction regarding confidentiality to

1 employees and agents handling files containing Medical Information, and security systems restricting
2 access to files containing Medical Information. By their affirmative acts and inactions set forth above,
3 Defendants disclosed or permitted the disclosure of Medical Information to unauthorized third parties in
4 violation of this Section, as well as failed establish appropriate procedures to ensure the confidentiality
5 and protection from unauthorized use and disclosure of the Medical Information it had received.

6 90. PARKER-HANNIFIN is required under the CMIA to ensure that it maintains, preserves,
7 and stores Medical Information in a manner that preserves the confidentiality of the information
8 contained therein. (Cal. Civ. Code § 56.101(a) & 56.36(b).)

9 91. PARKER-HANNIFIN is required to create, maintain, preserve, store, abandon, destroy
10 or dispose of Medical Information in a non-negligent manner. (Cal. Civ. Code § 56.101(a).)

11 92. Under the CMIA, electronic health record systems or electronic medical record systems
12 are required to protect and preserve the integrity of electronic Medical Information. (Cal. Civ. Code §
13 56.101(b)(1)(A).) The term “electronic health record” or “electronic medical record” means an electronic
14 record of health-related information on an individual that is created, gathered, managed, and consulted
15 by authorized health care clinicians and staff. (Cal. Civ. Code § 56.101(c) as defined by 42 U.S.C. §
16 17921(5).)

17 93. Plaintiff and members of the Class are “Patients” as defined by Cal. Civ. Code section
18 56.05(j).

19 94. The information at issue in this action is “Medical Information” as that term is defined by
20 section 56.05(i) of the CMIA.

21 95. As described above, the actions or inactions of PARKER-HANNIFIN failed to preserve
22 the confidentiality of Medical Information, including but not limited to Plaintiff’s and Class members’
23 Personal and Medical Information. In addition, with respect to current or former enrollees of PARKER-
24 HANNIFIN’s Group Health Plan or a health plan sponsored by an entity acquired by PARKER-
25 HANNIFIN, the actions or inactions of PARKER-HANNIFIN failed to preserve the confidentiality of
26 Medical Information, including but not limited to: health plan enrollment information, health insurance
27 plan ID numbers, and dates of coverage, and for a smaller subset of individuals, dates of medical
28 coverage, dates of medical services, provider names, claims information and medical and clinical

1 treatment information either that, alone or in combination with other publicly available information,
2 reveals their identities.

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

6 97. Since the Conti ransomware group published the entirety of the almost 420 gigabytes of
7 data it exfiltrated onto the web to be downloaded freely, the data at issue herein was viewed and the
8 confidentiality and integrity of that data was breached, lost, not preserved, and not protected by
9 Defendants.

10 98. In violation of the CMIA, Defendants disclosed or permitted the disclosure of Medical
11 Information regarding Plaintiff and Class members without authorization to a third party. This disclosure
12 did not qualify for any of the exemptions set forth in Civil Code Section 56.10(b) or (c), which provide
13 limited bases for allowing unauthorized disclosures. This disclosure of Medical Information to
14 unauthorized individuals resulted from the affirmative actions and inactions of Defendants and their
15 employees, which allowed hackers from the Conti ransomware group to access, view and obtain the
16 Medical Information of tens of thousands of PARKER-HANNIFIN or subsidiary employees or their
17 dependents.

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

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

23 101. In violation of the CMIA, PARKER-HANNIFIN's electronic health record systems or
24 electronic medical record systems did not protect and preserve the integrity of Plaintiff's and Class
25 members' Medical Information.

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

28 103. In violation of the CMIA, Defendants failed to give prompt, timely and fulsome notice of

1 the Conti ransomware attack and resulting data breach.

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

6 105. Plaintiff and members of the Medical Information Sub-class are therefore entitled to
7 injunctive relief, actual damages, statutory damages of \$1,000 per sub-Class member, punitive damages
8 of \$3,000 per sub-Class member, and reasonable attorneys' fees of \$1,000 per sub-Class Member and
9 costs.

10 **THIRD CAUSE OF ACTION**

11 **Invasion of Privacy**

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

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

14 107. The California Constitution provides: "All people are by nature free and independent and
15 have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possession,
16 and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const., Art. I.,
17 § 1.

18 108. Plaintiff and Class members had a legitimate expectation of privacy in their Personal
19 Information and Medical Information, and were entitled to the protection of this information against
20 disclosure to unauthorized third parties.

21 109. Defendants owed a duty to Plaintiff and Class members to keep their Personal Information
22 and Medical Information confidential.

23 110. Defendants failed to protect and released to unauthorized third parties the non-redacted
24 and non-encrypted Personal Information and Medical Information, of Plaintiff and Class members.

25 111. Defendants allowed unauthorized and unknown third parties access to and examination of
26 the Personal Information and Medical Information of Plaintiff and Class members by way of Defendants'
27 affirmative actions and negligent failures to protect this information.

28 112. The unauthorized release to, custody of, and examination by unauthorized third parties of

1 the Personal Information and Medical Information of Plaintiff and Class members is highly offensive to
2 a reasonable person.

3 113. The intrusion at issue was into a place or thing, which was private and is entitled to be
4 private. Plaintiff and Class members disclosed their Personal Information and Medical Information to
5 Defendants as part of Plaintiff's and Class members' relationships with Defendants, but privately and
6 with the intention that the Personal Information and Medical Information would be kept confidential and
7 would be protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their
8 belief that such information would be kept private and would not be disclosed without their authorization.

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

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

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

18 117. As a proximate result of the above acts and omissions of Defendants, the Personal
19 Information and Medical Information, of Plaintiff and Class members was disclosed to third parties
20 without authorization, causing Plaintiff and Class members to suffer injuries and damages in an amount
21 according to proof.

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

25 119. This action, if successful, will enforce an important right affecting the public interest and
26 would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons and/or
27 the general public. Private enforcement is necessary and places a disproportionate financial burden on
28 Plaintiff in relation to Plaintiff's stake in the matter. Because this case is brought for the purposes of

1 enforcing important rights affecting the public interest, Plaintiff also seeks the recovery of attorneys' fees
2 and costs in prosecuting this action against Defendants under Code of Civil Procedure section 1021.5
3 and other applicable law.

4 **FOURTH CAUSE OF ACTION**

5 **Violation of the Unfair Competition Law**

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

7 120. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein,
8 except all claims as to entitlement to damages.

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

12 122. Defendants engaged in "unlawful" business acts and practices in violation of the
13 California statutes set forth above, including Civil Code sections 56.10(a), 56.10(e), 56.20, 56.101,
14 1798.100 *et seq.*, 1798.21, 1798.29 § 1798.100 *et seq.*, and Article I, § 1 of the California Constitution.
15 Defendants acts also violated federal statutes and regulations, including the Federal Trade Commission
16 Act (15 U.S.C. § 45 *et seq.*), Health Insurance Portability and Accountability Act ("HIPAA") (45 C.F.R.
17 § 160.102), the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A
18 and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule
19 ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160
20 and Part 164, Subparts A and C and the other sections identified above. Plaintiff reserves the right to
21 allege other violations of law committed by Defendants that constitute unlawful business acts or practices
22 within the meaning of California Business & Professions Code sections 17200, *et seq.*

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

- 27 (a) does the practice offend an established public policy, which here are whether the practices
28 at issue offend the policies of protecting consumers' Personal Information and Medical

1 Information by engaging in illegal practices, as reflected in California law and policy set
2 forth above;

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

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

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

22 125. Defendants either knew or should have known that PARKER-HANNIFIN's data security
23 and protection practices were inadequate to safeguard the Personal Information and Medical Information
24 of Plaintiff and Class members, deter hackers, and detect a ransomware attack and resulting data breach
25 within a reasonable time, even though the risk of a data breach or theft was highly likely, especially given
26 Defendants had been on notice for almost a year of the potential for a Conti ransomware attack on its
27 systems. The business acts and practices by Defendants for failure to keep confidential medical or
28 personal data protected, encrypted and without sufficient security to be breached by an adverse third

1 party did not meet all applicable standards of care and vigilance. Thousands of individuals are now prime
2 targets for fraud, extortion, or access to other completely private information that would never have been
3 provided to Defendants if the patients or consumers knew how negligent or reckless Defendants would
4 be in not protecting such deeply personal medical and financial information private.

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

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

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

22 129. Pursuant to Business & Professions Code section 17203, Plaintiff seeks an order of this
23 Court both for himself, members of the Class and for the benefit of the public for injunctive relief in the
24 form of requiring Defendants to correct their illegal conduct, to prevent Defendants from repeating the
25 illegal and wrongful practices as alleged above and protect and preserve confidentiality of Personal
26 Information and Medical Information in Defendants' possession that has been accessed, downloaded,
27 exfiltrated, stolen, and viewed by at least one unauthorized third party because of Defendants' illegal and
28 wrongful practices set forth above.

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

8 **FIFTH CAUSE OF ACTION**

9 **Declaratory Relief**

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

11 132. A present and actual controversy exists between the parties. Defendants have failed to
12 acknowledge the wrongful nature of their actions, have not sent affected patients comprehensive data
13 breach notices regarding the Conti ransomware attack and Data Breach at issue herein, nor publicly
14 issued comprehensive corrective notices. Based on their inadequate disclosures to date, there is also no
15 reason to believe that Defendants have taken adequate measures to correct or enact adequate privacy
16 policies and revised their IT and computer systems to protect and preserve Plaintiff's and the Class
17 members' Personal Information and Medical Information in Defendants' possession.

18 133. Now that Defendants' insufficient information security is known to hackers, the Personal
19 Information and Medical Information in Defendants' possession is even more vulnerable to cyberattack.

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

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

26 136. Plaintiff and the Class members seek an order of this Court for declaratory, equitable
27 and/or injunctive relief in the form of an order finding Defendants have failed and continue to fail to
28 adequately protect Plaintiff's and the Class members' Personal Information and Medical Information

1 from release to unknown and unauthorized third parties, requiring Defendants to correct or enact adequate
2 privacy policies and security measures to protect and preserve Plaintiff's and the Class members'
3 Personal Information and Medical Information in their possession, and requiring Defendants to publicly
4 issue comprehensive corrective notices to Plaintiff, Class members and the public.

5 **PRAYER FOR RELIEF**

6 **WHEREFORE**, Plaintiff, both individually and on behalf of the Class and for the benefit of the
7 public as applicable, prays for orders and judgment in favor of Plaintiff and against Defendants as
8 follows, as applicable to the above Causes of Action:

- 9 A. Finding that this action satisfies the prerequisites for maintenance as a class action and
10 certifying the Class defined herein;
- 11 B. Designating Plaintiff as representative of the Class and his counsel as Class counsel;
- 12 C. Declaring Defendants' conduct in violation of the laws set forth above, including
13 California Civil Code sections 56.10(a), 56.10(e), 56.20, 56.101, 1798.150(a), 1798.82,
14 Business and Professions Code § 17200 *et seq.*, and Article I, § 1 of the California
15 Constitution.
- 16 D. An order:
- 17 1. prohibiting Defendants from engaging in the wrongful and unlawful acts described
18 herein;
- 19 2. prohibiting Defendants from refusing to send all affected persons updated and
20 comprehensive data breach notices regarding the ransomware attack and data theft
21 at issue herein in the form and timing required by law, and publicly issue
22 comprehensive corrective notices to Plaintiff, Class members and the public;
- 23 3. prohibiting Defendants from failing to protect, including through encryption, all
24 data collected through the course of their business operations in accordance with
25 all applicable regulations, industry standards, and federal and state laws;
- 26 4. prohibiting Defendants from refusing to implement and maintain a comprehensive
27 Information Security Program designed to protect the confidentiality and integrity
28 of the Personal Information and Medical Information of Plaintiff and the Class

1 members;

- 2 5. prohibiting Defendants from refusing to engage independent third-party security
3 auditors/penetration testers as well as internal security personnel to run automated
4 security monitoring, database scanning and security checks and conduct testing,
5 including simulated attacks, penetration tests, and audits on Defendants' systems
6 on a periodic basis, and ordering Defendants to promptly correct any problems or
7 issues detected by such third-party security auditors;
- 8 6. prohibiting Defendants from refusing to audit, test, and train security personnel
9 regarding any new or modified procedures;
- 10 7. requiring Defendants to segment data by, among other things, creating firewalls
11 and access controls so that if one area of Defendants' network is compromised,
12 hackers cannot gain access to other portions of Defendants' systems;
- 13 8. prohibiting Defendants from refusing to establish an information security training
14 program that includes at least annual information security training for all
15 employees, with additional training to be provided as appropriate based upon the
16 employees' respective responsibilities with handling personal identifying
17 information, as well as protecting the personal identifying information of Plaintiff
18 and Class members and infiltration of Defendants' computer system by phishing
19 processes by using such steps such as multi-factor authentication;
- 20 9. prohibiting Defendants from refusing to routinely and continually conduct internal
21 training and education, and inform internal security personnel how to immediately
22 identify and contain a ransomware attack or data breach when it occurs and what
23 to do in response to a breach; and,
- 24 10. prohibiting Defendants from refusing to implement, maintain, regularly review,
25 and revise as necessary a threat management program designed to appropriately
26 monitor Defendants' information networks for threats, both internal and external,
27 and assess whether monitoring tools are appropriately configured, tested, and
28 updated;

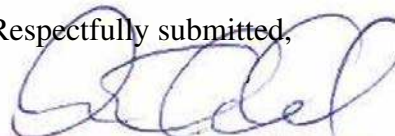
- 1 E. Awarding Plaintiff and the Class Members all actual, compensatory, statutory, punitive
2 and other damages, restitution and/or restitutionary disgorgement to which they are
3 entitled under the causes of action set forth above;
- 4 F. Awarding Plaintiff's counsel reasonable attorneys' fees and non-taxable expenses and
5 costs;
- 6 G. Awarding pre- and post-judgment interest at the maximum rate permitted by applicable
7 law; and,
- 8 H. Granting such further relief as the Court deems just.

9 **JURY DEMANDED**

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

11 Dated: June 2, 2022

Respectfully submitted,



12 **WHATLEY KALLAS, LLP**

13 Alan M. Mansfield, SBN: 125998

14 16870 W. Bernardo Drive

15 Suite 400

16 San Diego, CA 92127

17 Phone: (619) 308-5034

18 Fax: (888) 341-5048

19 Email: amansfield@whatleykallas.com

20 **WHATLEY KALLAS, LLP**

21 Joe R. Whatley, Jr. (*Pro Hac Vice application to
22 be filed*)

23 jwhatley@whatleykallas.com

24 Edith M. Kallas (*Pro Hac Vice application to be
25 filed*)

26 ekallas@whatleykallas.com

27 Patrick J. Sheehan (*Pro Hac Vice application to be
28 filed*)

psheehan@whatleykallas.com

152 W. 57th Street, 41st Floor

New York, NY 10019

Tel: (212) 447-7060

Fax: (800) 922-4851

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

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