POTTER HANDY LLP
Mark D. Potter (SBN 166317)
mark@potterhandy.com
James M. Treglio (SBN 228077)
jimt@potterhandy.com
8033 Linda Vista Rd, Suite 200
San Diego, CA 92111
Tel: (858) 375-7385
Fax: (888) 422-5191

Attorneys for Plaintiff JEANPAUL MAGALLANES, on behalf of himself and all others similarly situated,

30-2021-01213556-CU-MC-CXC

Assigned for all Purposes

Judge Glenda Sanders

cx-101

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ORANGE

JEANPAUL MAGALLANES, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

DISCOVERY PRACTICE MANAGEMENT, INC., a California Corporation; and DOES 1 through 100, inclusive,

Defendants.

CLASS ACTION

CLASS COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF (FOR VIOLATIONS OF:

(1) THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT, CIVIL CODE §§ 56, *ET SEQ*.);
(2) CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §17200, *et seq.*;
(3) CALIFORNIA CONSUMER RECORDS ACT, Cal. Civ. Code § 1798.82, *et seq.*

DEMAND FOR JURY TRIAL

Class Representative Plaintiff JEAN PAUL MAGALLANES ("Class Representative Plaintiff"), and by and through his attorneys, individually and on behalf of others similarly situated, alleges upon information and belief as follows:

I.

INTRODUCTION

1. Under the Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq.* (hereinafter referred to as the "Act"), Plaintiff JEANPAUL MAGALLANES ("Plaintiff"), and all other persons similarly situated, had a right to keep their personal medical information provided to Defendant DISCOVERY PRACTICE MANAGEMENT, INC. ("Discovery" or "Defendant") confidential. The short title of the Act states, "The Legislature hereby finds and declares that persons receiving health care services have a right to expect that the confidentiality of individual identifiable medical information derived by health service providers be reasonably preserved. It is the intention of the Legislature in enacting this act, to provide for the confidentiality of individually identifiable medical information, while permitting certain reasonable and limited uses of that information." The Act specifically provides that "a provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization...." Civil Code. § 56.10(a). The Act further provides that "Every provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical records shall be subject to the remedies ... provided under subdivisions (b) ... of Section 56.36." Civil Code § 56.101(a).

2. Civil Code § 56.36(b) provides Plaintiff, and all other persons similarly situated, with a private right to bring an action against Defendant for violation of Civil Code § 56.101 by specifically providing that "[i]n addition to any other remedies available at law, any individual may

bring an action against any person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: (1) ... nominal damages of one thousand dollars ($1,000). In order to recover under this paragraph, *it shall not be necessary that the plaintiff suffered or was threatened with actual damages*. (2) The amount of actual damages, if any, sustained by the patient." (Emphasis added.)

3. This class action is brought on behalf of Plaintiff and a putative class defined as all patients of Defendant who received care at Defendant's facility, satellite, or urgent care locations on or before June 26, 2020, and who received notices from Defendant that their information was compromised ("Breach Victims," the "Class," or the "Class Members").

4. As alleged more fully below, Defendant created, maintained, preserved, and stored Plaintiff's and the Class members' personal medical information onto the Defendant's computer network prior to June 26, 2020. Due to Defendant's mishandling of personal medical information recorded onto the Defendant's computer network, there was an unauthorized release of Plaintiff's and the Class members' confidential medical information that occurred continuously from approximately June 22, 2020, in violation of Civil Code § 56.101 of the Act.

5. As alleged more fully below, Defendant negligently created, maintained, preserved, and stored Plaintiff's and the Class members' confidential medical information in a non-encrypted format onto a data server which became accessible to an unauthorized person by logging in to two of Defendant's staff email accounts, without Plaintiff's and the Class members' prior written authorization. This act of providing unauthorized access to Plaintiff's and the Class Members' confidential medical information onto the internet continuously constitutes an unauthorized release of confidential medical information in violation of Civil Code § 56.101 of the Act. Because Civil Code § 56.101 allows for the remedies and penalties provided under Civil Code § 56.36(b), Class Representative Plaintiff, individually and on behalf of others similarly situated, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1). Additionally, Class Representative Plaintiff, individually and on behalf of others similarly situated, seeks injunctive relief for unlawful violations of Business and Professions Code §§ 17200, *et seq*.

6. Class Representative Plaintiff does not seek any relief greater than or different from the relief sought for the Class of which Plaintiff is a member. The action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons. Private enforcement is necessary and places a disproportionate financial burden on Class Representative Plaintiff in relation to Class Representative Plaintiff's stake in the matter.

II.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action under California Code of Civil Procedure § 410.10. The aggregated amount of damages incurred by Plaintiff and the Class exceeds the $25,000 jurisdictional minimum of this Court. The amount in controversy as to the Plaintiff individually and each individual Class member does not exceed $75,000, including interest and any pro rata award of attorneys' fees, costs, and damages. Venue is proper in this Court under California Bus. & Prof. Code § 17203, Code of Civil Procedure §§ 395(a) and 395.5 because Defendant does business in the State of California and in the County of Orange. Defendant has obtained medical information in the transaction of business in the County of Orange, which has caused both obligations and liability of Defendant to arise in the County of Orange.

III.

PARTIES

A. PLAINTIFF

8. Class Representative Plaintiff JEANPAUL MAGALLANES is a resident of the State of California. At all times relevant, Plaintiff MAGALLANES was a patient of Defendant who received medical treatment from Defendant, and was a patient, as defined by Civil Code § 56.05(k). Plaintiff's individual identifiable medical information derived by Defendant in electronic form was in possession of Defendant, including but not limited to Plaintiff's medical history, mental or physical condition, or treatment, including diagnosis and treatment dates. Such medical information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as Plaintiff's name, date of birth, addresses, medical record

number, insurance provider, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals Plaintiff's identity. Since receiving treatment at Defendant's facilities, Plaintiff MAGALLANES has received numerous solicitations by mail from third parties at an address he only provided to Defendant.

9. PLAINTIFF received from Defendant a notification that his personal medical information and their personal identifying information were disclosed when an unauthorized person logged in to two of Defendant's staff email accounts.

B. DEFENDANT

10. Defendant Discovery Practice Management, Inc. is a California corporation, with its principal places of business located at 4281 Katella Avenue, Suite 111, Los Alamitos, CA 90720. At all times relevant, Defendant is a "provider of health care" as defined by Civil Code § 56.05(m). Prior to June 26, 2020, Defendant created, maintained, preserved, and stored Plaintiff's and the Class members' individually identifiable medical information onto Defendant's computer network, including but not limited to Plaintiff's and the Class members' medical history, mental or physical condition, or treatment, including diagnosis and treatment dates. Such medical information included or contained an element of personal identifying information sufficient to allow identification of the individual, such as Plaintiff's and the Class members' names, dates of birth, addresses, medical record numbers, insurance providers, electronic mail addresses, telephone numbers, or social security numbers, or other information that, alone or in combination with other publicly available information, reveals Plaintiff's and the Class members' identities.

C. DOE DEFENDANTS

11. The true names and capacities, whether individual, corporate, associate, or otherwise, of Defendants sued herein as DOES 1 through 100, inclusive, are currently unknown to the Plaintiff, who therefore sue the Defendants by such fictitious names under the Code of Civil Procedure § 474. Each of the Defendants designated herein as a DOE is legally responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of court and/or amend this complaint to reflect the true names and capacities of the Defendants designated hereinafter as DOES 1 through

100 when such identities become known. Any reference made to a named Defendant by specific name or otherwise, individually or plural, is also a reference to the actions or inactions of DOES 1 through 100, inclusive.

D. AGENCY/AIDING AND ABETTING

12. At all times herein mentioned, Defendants, and each of them, were an agent or joint venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

13. Defendants, and each of them, aided and abetted, encouraged and rendered substantial assistance to the other Defendants in breaching their obligations to Plaintiff and the Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially assist the commissions of these wrongful acts and other wrongdoings complained of, each of the Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals, and wrongdoing.

IV.

FACTUAL ALLEGATIONS

A. The Data Breach

14. On or around July 1, 2021, Defendant issued a letter (the "Notice") to individuals, including Plaintiff, providing, for the first time, a notice of "an incident involving unauthorized access to that email environment" that Defendant maintains for the Authentic Recovery Center and Cliffside Malibu facilities ("Facilities") and which contained some information relating to certain individuals.

15. In the Notice, Defendant notified consumers that on July 31, 2020—***almost a year earlier***—its "investigation into suspicious email account activity identified unauthorized logins to tow Facilities' staff email accounts between June 22 and June 26, 2020" (the "Data Breach")—***or more than one year before Defendant sent the Notice.*** .

16. The Notice went on to say that after its investigation, Defendant confirmed (with assistance from a computer forensic firm) that Personal and Medical Information of certain individuals, including Plaintiff, were contained within the email accounts.

17. Yet, despite knowing many patients were in danger, Defendant did nothing to warn Breach Victims until 335 days later—a delay of almost a year after it discovered the Data Breach, or 374 days or more than a year after the actual date of the Data Breach, an unreasonable amount of time under any objective standard. During this time, cyber criminals had free reign to surveil and defraud their unsuspecting victims. Defendant apparently chose to complete its internal investigation and develop its excuses and speaking points before giving class members the information they needed to protect themselves against fraud and identity theft.

18. After its "comprehensive review of the accounts," Defendant determined that:

> The information involved may include your name, address, date of birth, medical record and/or patient account number and/or clinical information, such as diagnosis, treatment information, and/or prescription information.

This was a staggering coup for cyber criminals and a stunningly bad showing for Defendant.

19. It is apparent from Defendant's Notice that the Personal and Medical information contained within the server was not encrypted.

20. In spite of the severity of the Data Breach, Defendant has done very little to protect Breach Victims. In the Notice, Defendant states that it is notifying Breach Victims and as a precaution, it recommends review of statements received from healthcare providers and to contact the provider immediately if charges for services not received are reflected therein. In effect, shirking its responsibility for the harm it has caused and putting it all on the Breach Victims.

21. Defendant failed to adequately safeguard Plaintiff and Class members' Personal and Medical Information, allowing cyber criminals to access this wealth of priceless information and use it for more than a year before Defendant warned the criminals' victims, the Breach Victims, to be on the lookout.

22. Defendant failed to spend sufficient resources on monitoring external incoming emails and training its employees to identify email-born threats and defend against them.

23. Defendant had obligations created by the Health Insurance Portability and Accountability Act ("HIPAA"), the Confidentiality of Medical Information Act ("CMIA"), reasonable industry standards, its own contracts with its patients and employees, common law, and its representations to Plaintiff and Class members, to keep their Personal and Medical Information confidential and to protect the information from unauthorized access.

24. Plaintiff and Class members provided their Personal and Medical Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

25. Indeed, as discussed below, Defendant promised Plaintiff and Class members that it would do just that.

B. Defendant Expressly Promised to Protect Personal and Medical Information

26. Defendant provides all patients, including Plaintiff and Class members, its Notice of Privacy Practices, which states that:

> Discovery Practice Management ("Discovery") uses health information about you for treatment, to obtain payment for treatment, to evaluate the quality of care you receive, and for other administrative and operational purposes. Your health information is contained in a medical record that is the physical property and responsibility of Discovery…..[1]

27. Likewise, Defendant, as part of its Notice of Privacy Practices, provides every patient a section on "Your Rights Regarding your Protected Health Information:" that assures the patients of their right to the confidentiality of all their records provided to, generated by, or retained by Defendant:

> 1. You have the right to request a restriction of your PHI. You have the right to ask for restrictions on the ways in which we use and disclose your PHI for purposes of treatment, payment or health care operations. You may also request that any part of your PHI not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice. Your request must state the specific restriction requested and to whom you want the restriction to apply. We are not required to agree to a restriction that you request, except we must agree not to disclosure your PHI to your health plan if the disclosure (1) is for payment or health care operations purposes and is not otherwise required by law, and (2) the

[1] Discovery Practice Management, Inc., "Notice of Privacy Practices," Effective Date: March 1, 2017, https://centerfordiscovery.com/privacy-policy/

> disclosure deals solely with health care items or services that were paid for in full by a person or entity other than your health plan. For example, if you paid out-of-pocket in full for a service, we must agree to your request to restrict disclosure of that information to your health plan.….[2]

28. Notwithstanding the foregoing assurances and promises, Defendant failed to protect the Personal and Medical Information of Plaintiff and other Class members from cyber criminals using relatively unsophisticated means to dupe its patients, as conceded in the Notice.

29. If Defendant truly understood the importance of safeguarding patients' Personal and Medical Information, it would acknowledge its responsibility for the harm it has caused, and would compensate class members, provide long-term protection for Plaintiff and the Class, agree to Court-ordered and enforceable changes to its cybersecurity policies and procedures, and adopt regular and intensive training to ensure that a data breach like this never happens again.

30. Defendant's data security obligations were particularly important given the known substantial increase in data breaches in the healthcare industry, including the recent massive data breach involving Fairchild Medical Center, Scripps Health, HealthNet, LabCorp, Quest Diagnostics, and American Medical Collections Agency. And given the wide publicity given to these data breaches, there is no excuse for Defendant's failure to adequately protect Plaintiff and Class members' Personal and Medical Information.

31. That information, is now in the hands of cyber criminals who will use it if given the chance. Much of this information is unchangeable and loss of control of this information is remarkably dangerous to consumers.

C. Defendant had an Obligation to Protect Personal and Medical Information under Federal and State Law and the Applicable Standard of Care

32. Defendant is an entity covered by HIPAA (45 C.F.R. § 160.102). As such, it is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[2] *Id.*

33. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

34. HIPAA's Security Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is held or transferred in electronic form.

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

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

37. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

38. HIPAA also required Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

39. HIPAA also required Defendant to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

40. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[3]

41. Defendant was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

42. As described before, Defendant is also required (by the California Consumer Records Act ("CCRA"), CMIA and various other states' laws and regulations) to protect Plaintiff's and Class members' Personal and Medical Information, and further, to handle any breach of the same in accordance with applicable breach notification statutes.

43. In addition to their obligations under federal and state laws, Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal and Medical Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Breach Victims to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Personal and Medical Information of the Breach Victims.

44. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to design, maintain, and test its computer systems and email system to ensure that the Personal and Medical Information in Defendant's possession was adequately secured and protected.

[3] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for professionals/breach-notification/index.html (emphasis added).

45. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to create and implement reasonable data security practices and procedures to protect the Personal and Medical Information in their possession, including adequately training its employees and others who accessed Personal Information within its computer systems on how to adequately protect Personal and Medical Information.

46. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to implement processes that would detect a breach on its data security systems in a timely manner.

47. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to act upon data security warnings and alerts in a timely fashion.

48. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to adequately train and supervise its employees to identify and avoid any phishing emails that make it past its email filtering service.

49. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to disclose if its computer systems and data security practices were inadequate to safeguard individuals' Personal and Medical Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal and Medical Information with Defendant.

50. Defendant owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendant to disclose in a timely and accurate manner when data breaches occurred.

51. Defendant owed a duty of care to Breach Victims because they were foreseeable and probable victims of any inadequate data security practices.

//

//

//

//

//

D. A Data Breach like Defendant's Results in Debilitating Losses to Consumers

52. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[4] Cyber criminals can leverage Plaintiff's and Class members' Personal and Medical Information that was stolen in the Data Breach to commit thousands-indeed, millions-of additional crimes, including opening new financial accounts in Breach Victims' names, taking out loans in Breach Victims' names, using Breach Victims' names to obtain medical services and government benefits, using Breach Victims' Personal Information to file fraudulent tax returns, using Breach Victims' health insurance information to rack up massive medical debts in their names, using Breach Victims' health information to target them in other phishing and hacking intrusions based on their individual health needs, using Breach Victims' information to obtain government benefits, filing fraudulent tax returns using Breach Victims' information, obtaining driver's licenses in Breach Victims' names but with another person's photograph, and giving false information to police during an arrest. Even worse, Breach Victims could be arrested for crimes identity thieves have committed.

53. Personal and Medical Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years.

54. This was a financially motivated data breach, as the only reason cyber criminals stole Plaintiff's and the Class members' Personal and Medical Information from Defendant was to engage in the kinds of criminal activity described above, which will result, and has already begun to, in devastating financial and personal losses to Breach Victims.

55. This is not just speculative. As the FTC has reported, if hackers get access to Personal and Medical Information, they ***will*** use it.[5]

[4] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[5] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

56. Hackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information **may continue for years**. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[6]

57. For instance, with a stolen social security number, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[7] Identity thieves can also use the information stolen from Breach Victims to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills.

58. Medical identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more "than identity thefts involving banking and finance, the government and the military, or education."[8]

59. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[9]

60. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can

---

[6] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu (emphasis added).

[7] *See, e.g.*, Christine Di Gangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with- your-social-security-number-108597/.

[8] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

[9] *Id.*

be, say, five dollars or more where PHI can go from $20 say up to—we've seen $60 or $70 [(referring to prices on dark web marketplaces)]."[10] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[11]

61. If, moreover, the cyber criminals also manage to steal financial information, credit and debit cards, health insurance information, driver's licenses and passports there is no limit to the amount of fraud that Defendant has exposed the Breach Victims to.

62. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[12] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[13]

63. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[14]

64. The danger of identity theft is compounded when a minor's Personal and Medical Information is compromised because minors typically have no credit reports to monitor. Thus, it can be difficult to monitor because a minor cannot simply place an alert on their credit report or "freeze" their credit report when no credit report exists.

---

[10] ID Experts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, https://www.idexpertscorp.com/knowedge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat

[11] *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from The Global State of Information Security Survey 2015,https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global- state-of-information-security-survey-2015.pdf

[12] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[13] *Id.*; *see also Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[14] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

65. Defendant did not even bother to offer identity monitoring to Plaintiff and the Class. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal and Medical Information is stolen and when it is used. Even if it did, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Personal and Medical Information)—it does not prevent identity theft.[15] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

66. As a direct and proximate result of the Data Breach, Plaintiff and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

67. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Personal and Medical Information;

b. Improper disclosure of their Personal and Medical Information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal and Medical Information being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

[15] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the- cost.html.

e. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their Personal and Medical Information and that fraudsters have already used that information to initiate spam calls to members of the Class;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of customers' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal and Medical Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

68. Moreover, Plaintiff and Class have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

69. Despite acknowledging the harm caused by the Data Breach on Plaintiff and Class members, Defendant does nothing to reimburse Plaintiff and Class members for the injuries they have already suffered.

V.

CLASS ACTION ALLEGATIONS

70. Class Representative Plaintiff brings this action on his own behalf and on behalf of all other persons similarly situated. The putative class that Class Representative Plaintiff seeks to represent is composed of:

> All patients of Defendant who received treatment at one of Defendant's facilities, satellite, or urgent care locations on or before June 26, 2020, and who received notice from Defendant that their information was compromised (hereinafter the "Class").

Excluded from the Class are the natural persons who are directors, and officers, of the Defendant. Class Representative Plaintiff expressly disclaims that he is seeking a class-wide recovery for personal injuries attributable to Defendant's conduct.

71. Plaintiff is informed and believes that the total number of Class Members exceeds 50,000 persons, and as such, the members of the Class are so numerous that joinder of all members is impracticable. While the exact number of the Class members is unknown to Class Representative Plaintiff at this time, such information can be ascertained through appropriate discovery, from records maintained by Defendant.

72. There is a well-defined community of interest among the members of the Class because common questions of law and fact predominate, Class Representative Plaintiff's claims are typical of the members of the class, and Class Representative Plaintiff can fairly and adequately represent the interests of the Class.

73. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class are:

(a) Whether Defendant failed to adequately safeguard Plaintiff's and the Class' Personal and Medical Information;

(b) Whether Defendant failed to protect Plaintiff's and the Class' Personal and Medical Information;

(c) Whether Defendant's email and computer systems and data security practices used to protect Plaintiff's and the Class' Personal and Medical Information violated the FTC Act, HIPAA, CMIA, CCRA and/or Defendant's other duties;

(d) Whether Defendant violated the data security statutes and data breach notification statutes applicable to Plaintiff and the Class;

(e) Whether Defendant failed to notify Plaintiff and members of the Class about the Data Breach expeditiously and without unreasonable delay after the Data Breach was discovered;

(f) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Breach Victims' Personal and Medical Information properly and as promised;

(g) Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class' Personal and Medical Information, including whether its conduct constitutes negligence *per se*;

(h) Whether Defendant entered into implied contracts with Plaintiff and the members of

the Class that included contract terms requiring Defendant to protect the confidentiality of Personal and Medical Information and have reasonable security measures;

(i) Whether Defendant violated the consumer protection statutes, data breach notification statutes, and state medical privacy statutes applicable to Plaintiff and the Class;

(j) Whether Defendant failed to notify Plaintiff and Breach Victims about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

(k) Whether Defendant's conduct described herein constitutes a breach of their implied contracts with Plaintiff and the Class;

(l) Whether Plaintiff and the members of the Class are entitled to damages as a result of Defendant's wrongful conduct;

(m) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

(n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class.

Class Representative Plaintiff's claims are typical of those of the other Class members because Class Representative Plaintiff, like every other Class member, was exposed to virtually identical conduct and is entitled to nominal damages of one thousand dollars ($1,000) per violation pursuant to Civil Code §§ 56.101 and 56.36(b)(1).

74. Class Representative Plaintiff will fairly and adequately protect the interests of the Class. Moreover, Class Representative Plaintiff has no interest that is contrary to or in conflict with those of the Class he seeks to represent during the Class Period. In addition, Class Representative Plaintiff has retained competent counsel experienced in class action litigation to further ensure such protection and intend to prosecute this action vigorously.

75. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for the Defendant in the State of California and would lead to repetitious trials of the numerous common questions of fact and law in the State of California. Class Representative Plaintiff knows of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action. As a result, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

76. Proper and sufficient notice of this action may be provided to the Class members through direct mail.

77. Moreover, the Class members' individual damages are insufficient to justify the cost of litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Absent certification of this action as a class action, Class Representative Plaintiff and the members of the Class will continue to be damaged by the unauthorized release of their individual identifiable medical information.

VI.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

(Violations of the Confidentiality of Medical Information Act, Civil Code § 56, *et seq.*)
(Against All Defendants)

78. Plaintiff and the Class incorporate by reference all of the above paragraphs of this Complaint as though fully stated herein.

79. Defendant is a "provider of health care," within the meaning of Civil Code § 56.05(m), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), of "patients" of the Defendant, within the meaning of Civil Code § 56.05(k).

80. Plaintiff and the Class are "patients" of Defendant within the meaning of Civil Code § 56.05(k). Furthermore, Plaintiff and the Class, as patients of Defendant, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), stored onto Defendant's server, and received treatment at one of Defendant's facilities, satellite, or urgent care locations on or before June 26, 2020.

81. On or about July 31, 2020, Defendant determined that a misconfiguration existed involving Plaintiff's and Class members' individual identifiable "medical information," within the meaning of Civil Code § 56.05(j),[16] including Plaintiff's and the Class members' name, address,

[16] Pursuant to Civil Code § 56.05(j), "Medical information" means "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care...regarding a patient's medical history, mental or physical condition, or treatment. 'Individually Identifiable' means that the medical information includes or contains any elements of personal identifying information sufficient to allow identification of the

date of birth, medical record and/or patient account number and/or clinical information, such as diagnosis, treatment information, and/or prescription information.

82. Defendant was made aware of a suspicious email account activity in its servers. Defendant immediately commenced an investigation and began working with a computer forensic firm to determine the nature and scope of the issue. Defendant also immediately addressed the misconfiguration and took steps to secure the accounts. Defendant also conducted a comprehensive review of the accounts. Through the investigation, Defendant determined that there were unauthorized logins to two Facilities' staff email accounts between June 22 and June 26, 2020. On June 2, 2021, following an extensive review of forensic evidence associated with the server, Defendant's investigation determined that the information of certain individuals were contained within the email accounts.

83. As a result of Defendant's above-described conduct, Plaintiff and the Class have suffered damages from the unauthorized release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10 and 56.101.

84. Because Civil Code § 56.101 allows for the remedies and penalties provided under Civil Code § 56.36(b), Plaintiff individually and on behalf of the Class seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1); and Plaintiff individually seeks actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2).

SECOND CAUSE OF ACTION
(Violations of the CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §17200, *et seq.*)

85. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

---

individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." As alleged herein, Defendant's unencrypted email accounts contained Plaintiff's and the Class members' name, address, date of birth, medical record and/or patient account number and/or clinical information, such as diagnosis, treatment information, and/or prescription information, and thus contained individually identifiable medical information as defined by Civil Code § 56.05(j)

86. Defendant is both organized under the laws of California and headquartered in California. Defendant violated California's Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard their Personal and Medical Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that they did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the Class' Personal and Medical Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class' Personal and Medical Information;

b. by soliciting and collecting Class members' Personal and Medical Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class members' Personal and Medical Information in an unsecure electronic environment;

c. by failing to disclose the Data Breach in a timely and accurate manner, in violation of Cal. Civ. Code §1798.82;

d. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq.*;

e. by violating the CMIA, Cal. Civ. Code § 56, *et seq.*; and

f. by violating the CCRA, Cal. Civ. Code § 1798.82.

87. These unfair acts and practices were immortal, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class members. Defendant's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security

measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq.*, CMIA, Cal. Civ. Code § 56, *et seq.*, and the CCRA, Cal. Civ. Code § 1798.81.5.

88. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff and the Class were injured and lost money or property, including but not limited to the overpayments Defendant received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their Personal and Medical Information, and additional losses described above.

89. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and Class members' Personal and Medical Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

90. The conduct and practices described above emanated from California where decisions related to Defendant's advertising and data security were made.

91. Plaintiff seeks relief under the UCL, including restitution to the Class of money or property that the Defendant may have acquired by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

THIRD CAUSE OF ACTION
(Violations of the CALIFORNIA CONSUMER RECORDS ACT, Cal. Civ. Code § 1798.82, *et seq.*)

92. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

93. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized

person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

94. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

95. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

iii. If the information is possible to determine at the time the notice is provided, then any of the following:

1. The date of the breach;

2. The estimated date of the breach; or

3. The date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether notification was delayed as a result of law enforcement investigation, if that information is possible to determine at the time the notice is provided;

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

vi. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

96. The Data Breach described herein constituted a "breach of the security system" of Defendant.

97. As alleged above, Defendant unreasonably delayed informing Plaintiff and Class members about the Data Breach, affecting their Personal and Medical Information, after Defendant knew the Data Breach had occurred.

98. Defendant failed to disclose to Plaintiff and the Class, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Personal and Medical Information when Defendant knew or reasonably believed such information had been compromised.

99. Defendant's ongoing business interests gave Defendant incentive to conceal the Data Breach from the public to ensure continued revenue.

100. Upon information and belief, no law enforcement agency instructed Defendant that timely notification to Plaintiff and the Class would impede its investigation.

101. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and the Class were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and Class members because their stolen information would have had less value to identity thieves.

102. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and the Class suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

103. Plaintiff and the Class seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiff and the other Class members as alleged above and equitable relief.

104. Defendant's misconduct as alleged herein is fraud under Cal. Civ. Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant conducted with the intent on the part of Defendant of depriving Plaintiff and the Class of "legal rights or otherwise causing injury." In addition, Defendant's misconduct as alleged herein is malice or oppression under Cal. Civ. Code § 3294(c)(1) and (c) in that it was despicable conduct carried on by Defendant with a willful and conscious disregard of the rights or safety of Plaintiff and the Class and despicable conduct that has subjected Plaintiff and the Class to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiff and the Class are entitled to punitive damages against Defendant under Cal. Civ. Code § 3294(a).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the Court grant Plaintiff and the Class members the following relief against Defendant:

a. An order certifying this action as a class action under Code of Civil Procedure §382, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, including statutory damages under the CMIA, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein, including, but not limited to:

i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

iv. Ordering that Defendant's segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

vi. Ordering that Defendant conduct regular database scanning and securing checks;

vii. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

viii. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law, including the CCRA, Cal. Civ. Code § 1798.84(g), UCL, Cal. Bus. & Prof. Code § 17082, CMIA, Cal. Civ. Code 56.35; and

f. An award of such other and further relief as this Court may deem just and proper.

POTTER HANDY LLP

/s/ James M. Treglio

Dated: July 27, 2021 By: _____

Mark D. Potter, Esq.
James M. Treglio, Esq.
Attorneys for the Plaintiff and the Class

DEMAND FOR JURY TRIAL

Plaintiff and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

POTTER HANDY LLP

/s/ James M. Treglio

Dated: July 27, 2021 By: _____

Mark D. Potter, Esq.
James M. Treglio, Esq.
Attorneys for the Plaintiff and the Class