POTTER HANDY LLP
Mark D. Potter (SBN 166317)
mark@potterhandy.com
James M. Treglio (SBN 228077)
jimt@potterhandy.com
100 Pine St., Ste 1250
San Francisco, CA 94111
Tel: (415) 534-1911
Fax: (888) 422-5191

Attorneys for Plaintiff

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF RIVERSIDE

MARGIE LOPEZ, on behalf of herself and all others similarly situated,

Plaintiff,

vs.

CENCORA, INC., a Delaware corporation; and DOES 1 through 100, inclusive,

Defendants.

Case No.

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 CONSUMER PRIVACY ACT § 1798.150; and
(3) CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §17200, *et seq.*

DEMAND FOR JURY TRIAL

Class Representative Margie Lopez ("Class Representative" or "Plaintiff"), by and through her 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 and all other persons similarly situated, had a right to keep their personal medical information provided to Defendants Cencora, Inc. ("Cencora" or "Defendants") 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 Defendants 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 citizens of the State of California who provided their personal medical information to Defendants and/or their partner health plans on or before June 30, 2022, and who received notices from Defendants that their information was compromised ("Breach Victims," the "Class," or the "Class Members").

4. As alleged more fully below, Defendants created, maintained, preserved, and stored Plaintiff's and the Class members' personal medical information onto the Defendant's computer network prior to February 21, 2024. Due to Defendant's mishandling of personal medical information recorded onto the Defendants' computer network, there was an unauthorized release of Plaintiff's and the Class members' confidential medical information that occurred on or about February 21, 2024, in violation of Civil Code § 56.101 of the Act.

5. As alleged more fully below, Defendants 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, 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, 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).

6. The PII disclosed in the Data Breach is also protected by the California Consumer Privacy Act of 2018 ("CCPA"). For purposes of CCPA Section 1798.150, "personal information" is defined as an individual's first name or first initial and his or her last name in combination with

any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (1) social security number; (2) driver's license number or California ID card number; (3) account number or credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account; (4) medical information; and/or (5) health insurance information.[1]

7. Here, unencrypted names were revealed along with account information that would permit access to individuals' financial and other accounts across the web. According to Defendants' notice to affected customers dated May 17, 2024, the PII subjected to unauthorized access and exfiltration, theft, or disclosure in the Data Breach includes (among other things): "first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions." In combination, those pieces of PII could permit access to other accounts using similar or the same information, including financial accounts.

8. When nonencrypted and nonredacted personal information defined in Section 1798.150 is subjected to unauthorized access and exfiltration, theft, or disclosure by a company that has failed to maintain reasonable security measures, the CCPA explicitly authorizes private litigants to bring individual or class action claims.[2]

9. Defendants have failed to maintain reasonable security controls and systems appropriate for the nature of the PII it maintains as required by the CCPA and other common and statutory laws. According to one blogger for the International Association for Privacy Professionals, "encryption is a security strategy …[that] protects your organization from scenarios like a devastating breach where, if the adversary were to gain access to your servers, the data stored would be of no use to them, unless they have the encryption key. It's an all-or-nothing security posture: You either get to see the data unencrypted, or you don't."[3] "[O]rganizations should encrypt their

[1] In other sections of the CCPA, "personal information" is defined more broadly as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

[2] CCPA Section 1798.192 also states: "Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable."

[3] Tuow, Steve, Encryption, redaction and the CCPA, available at https://iapp.org/news/a/encryption-redaction-and-the-ccpa/ (last accessed July 14, 2022).

data on a disk as a required security measure. But they must not stop there. In fact, the CCPA is clear that they should go further." *Id.*

10. Defendants also failed to maintain proper measures to detect hacking and intrusion. According to its notice to affected customers, "On February 21, 2024, Cencora learned that data from its information systems had been exfiltrated…" However, it was only "On April 10, 2024, we confirmed that some of your personal information was affected by the incident." As explained below, Defendants should have had breach detection protocols in place. If they had, they could have learned of the breach and alerted customers much sooner and not almost three months after they discovered the Data Breach.

11. Nearly all "best practices" security frameworks, e.g., the U.S. National Institute of Standards and Technology's (NIST) Special Publication 800, require log aggregation, log monitoring, and automated intrusion detection systems that alert a company of unauthorized access or the anomalous use of hacked user accounts. Had Defendants properly deployed those industry standard systems, the breach might not have occurred or, if it had, Defendants would have promptly detected it.

12. Because (i) Defendants have failed to maintain reasonable security measures, and (ii) Defendants disclosed their customers' unencrypted names and birth dates, among others, the CCPA explicitly permits an individual or class action under Section 1798.150 for this Data Breach.

13. Defendants claim that "we are also working with cybersecurity experts to reinforce our systems and information security protocols in an effort to avoid incidents like this from occurring in the future." But the viewing, theft, and attempted sale of California consumers' PII on the dark web has already occurred and cannot be cured.

14. Defendants disregarded Plaintiff's and Class members' privacy rights in the PII by, among other things, (i) failing to implement reasonable security safeguards to prevent or timely detect the Data Breach; (ii) failing to detect the Data Breach when or after it occurred; (iii) failing to disclose to customers that it did not implement such reasonable security safeguards; and (iv) failing to provide sufficiently prompt, thorough, and accurate notice and information about the Data Breach.

15. As a result of the Data Breach, Plaintiff and the Classes have been injured in several ways. Plaintiff and Class members (i) now know or should know that their PII was hacked and put up for sale on the dark web for purchase by malicious actors; (ii) face an imminent and ongoing risk of identity theft and similar cybercrimes; (iii) have expended and will continue to expend time and money to protect against cybercrimes; (iv) have lost value in their PII; and (v) did not receive the benefit of their bargain with Defendant regarding data privacy.

16. Plaintiff and Class members are therefore (i) entitled to actual and statutory damages under the CCPA and other laws, (ii) have incurred actual and concrete damages as a result of the unauthorized sale of their PII to malicious actors on the dark web, and (iii) face ongoing risks of disclosure of their PII in subsequent data breaches because Defendants have not demonstrated that they have implemented reasonable security systems and procedures. Plaintiff and Class members have a significant interest in the protection and safe storage of their PII. They are therefore entitled to declaratory, injunctive, and other equitable relief necessary to protect their PII. This includes, but is not limited to, an order compelling Defendants to adopt reasonable security procedures and practices to safeguard customers' PII and prevent future data breaches.

17. Class Representative 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's stake in the matter.

II.

JURISDICTION AND VENUE

18. 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 Code of Civil Procedure §§ 395(a) and 395.5 because Defendants do business in the State of

California and in the County of Riverside. Defendants have obtained medical information in the transaction of business in the County of Riverside which has caused both obligations and liability of Defendants to arise in the County of Riverside.

III.

PARTIES

A. PLAINTIFF

19. Class Representative Margie Lopez is a resident of the State of California. At all times relevant, Plaintiff was registered with one of Defendants' partner companies, which Defendants helped facilitate access to therapies through drug distribution, patient support services, business analytics and technology, and other services. The information provided by Plaintiff to Defendants through Defendants' partner health plans included Plaintiff's medical information. Thus, Plaintiff was a patient, as defined by Civil Code § 56.05(k). Plaintiff's individual identifiable medical information derived by Defendants in electronic form was in possession of Defendants, 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 Defendants obtained Plaintiff's information, Plaintiff has received numerous solicitations by mail from third parties at an address she only provided to Defendants through their partner companies. Plaintiff has also received numerous alerts from her credit monitoring company that her email and password are now found on the dark web. Plaintiff began receiving these alerts on or about March 12, 2024 and she continues to receive them to date.

20. PLAINTIFF received from Defendants a notification that her personal medical information and personal identifying information were disclosed when an unauthorized person gained access to Defendants' servers.

B. DEFENDANT

21. Defendant Cencora, Inc. partners with pharmaceutical companies, pharmacies, and healthcare providers to facilitate access to therapies through drug distribution, patient support services, business analytics and technology, and other services. It is a Delaware corporation with its principal place of business located at 1 West First Avenue, Conshohocken, PA 19428. Defendants operate throughout the State of California including in Riverside, California. At all times relevant, Defendant is a "provider of health care" as defined by Civil Code § 56.05(m), or a contractor as defined by Civil Code §56.05(d). Prior to February 21, 2024, Defendants created, maintained, preserved, and stored Plaintiff's and the Class members' individually identifiable medical information onto Defendants' 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

22. 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 sues 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

23. 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.

24. 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

25. Defendants partner with pharmaceutical companies, pharmacies, and healthcare providers to facilitate access to therapies through drug distribution, patient support services, business analytics and technology, and other services. Defendants gather information in order to provide these services. With data stored regarding patients nationwide, Defendants collect a significant amount of sensitive data from patients, as delineated above.

26. In order to perform these functions, Defendants regularly collect information from their partner companies, including personally identifiable information and medical information, including the diagnosis and treatment plans. To that end, Defendants operate as either a contractor performing administrative functions, as described in Civil Code §§56.10 (d), 56.26, or a medical provider under Civil Code §56.05(m). Defendants are also considered a "recipient" of medical information as defined by Civil Code §56.13.

27. Whether deemed as a medical provider, contractor, administrator, or recipient, Defendants, who had access to mental health records (defined as "sensitive services" under Civil Code §56.05(n)), had an affirmative duty under Civil Code §§56.10 and 56.101 to not disclose the confidential medical record to anyone without proper authorization.

28. On or around May 17, 2024, Defendants issued a letter (the "Notice") to individuals, including Plaintiff, providing, for the first time, a notice of "an event that involved your personal information that Lash Group has through the patient support and access programs it manages on behalf of Bristol Myers Squibb and/or Bristol Myers Squibb Patient Assistance Foundation."

29. In the Notice, Defendants states that "On February 21, 2024, Cencora learned that data from its information systems had been exfiltrated, some of which could contain personal information. Upon initial detection of the unauthorized activity, Cencora immediately took containment steps and commenced an investigation with the assistance of law enforcement, cybersecurity experts and outside lawyers. On April 10, 2024, we confirmed that some of your personal information was affected by the incident." (the "Data Breach").

30. The Notice went on to say that "Based on our investigation, personal information was affected, including potentially your first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions." Defendants confirmed that some of Plaintiff's information were present in the files that were illegally accessed from Defendants' server. Defendants failed to state in their Notice when they identified that Plaintiff's information was included in the Data Breach. By definition, the information the Notice states was affected by the breach included confidential medical information regarding "sensitive services." as defined by Civil Code §56.05(i) and (n).

31. Beginning on or about March 12, 2024, Plaintiff began receiving notifications from her credit monitoring provider informing her that her email and password have been found on the dark web. To date, Plaintiff continues to receive such alerts.

32. Yet, despite knowing many patients were in danger, Defendants did nothing to warn Breach Victims until almost three months after they discovered the Data Breach and 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. Defendants apparently chose to complete their internal investigation and develop their excuses and speaking points before giving class members the information they needed to protect themselves against fraud and identity theft.

33. This was a staggering coup for cyber criminals and a stunningly bad showing for Defendants. And if those affected included minors, this data breach will likely affect them for their entire lives.

34. It is apparent from Defendants' Notice that the Personal and Medical information contained within the server was not encrypted or was inadequately protected.

35. In spite of the severity of the Data Breach, Defendants have done very little to protect Breach Victims. In the Notice, Defendants state that it is notifying Breach Victims and they encourage the Breach Victims to remain vigilant against incidents of identity theft and fraud, and to review their account statements and explanation of benefits forms, and to monitor their free credit reports for suspicious activity, and to detect errors. In effect, shirking their responsibility for the harm they caused and putting them all on the Breach Victims.

36. Defendants failed to adequately safeguard Plaintiff's and Class members' Personal and Medical Information, allowing cyber criminals to access this wealth of priceless information and use it for almost three months before Defendants warned the criminals' victims, the Breach Victims, to be on the lookout.

37. Defendants failed to spend sufficient resources on monitoring external incoming emails and training their employees to identify email-born threats and defend against them.

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

39. Plaintiff and Class members provided their Personal and Medical Information to Defendants with the reasonable expectation and mutual understanding that Defendants would

comply with their obligations to keep such information confidential and secure from unauthorized access.

40. Indeed, as discussed below, Defendants promised Plaintiff and Class members that they would do just that.

B. Defendants Expressly Promised to Protect Personal and Medical Information

41. Defendants provide all clients, including Plaintiff and Class members, their Privacy Statement, which states that:

> Security of Your Personal Data
>
> We use appropriate technical, administrative and physical safeguards to protect Personal Data from loss, misuse or alteration. We limit access to Personal Data to those employees, agents, contractors and other third parties who have a business need to know...[4]

42. Likewise, Defendants' State Supplement to Privacy Statement, which applies to individuals who reside in the State of California states that:

> Information We Collect, Disclose, or Sell
>
> Cencora has not sold or shared (as those terms are defined under applicable laws) Personal Data, including Sensitive Personal Data, to any third party in the last twelve (12) months. Where Cencora discloses Personal Data to third parties, it does so for the same business purposes described below and, where appropriate, requires that such parties maintain its confidentiality and maintain appropriate systems and processes to ensure its security and protection. …
>
> Cencora does not "sell" or "share" (within the meaning of the State Privacy Laws) Personal Data about you to third parties. Relatedly, we do not sell or share Personal Data of individuals under 16 years of age. Cencora does not use or disclose sensitive Personal Data, as defined in applicable laws, for any purposes other than those permitted by applicable law.
>
> Cencora does not use or disclose sensitive Personal Data for any purposes other than those permitted by applicable law.[5]

43. Notwithstanding the foregoing assurances and promises, Defendants failed to protect the Personal and Medical Information of Plaintiff and other Class members from cyber criminals

[4] Cencora, "Privacy Statement," https://www.cencora.com/global-privacy-statement, last visited on June 6, 2024.

[5] Cencora, "State Supplement to Privacy Statement," https://www.cencora.com/global-california-supplement, last visited on June 6, 2024.

using relatively unsophisticated means to dupe their patients, as conceded in the Notice to the Breach Victims.

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

45. Defendants' data security obligations were particularly important given the known substantial increase in data breaches, including the recent massive data breach involving PostMeds, Tri City Medical, Kaiser Foundation Health Plan, Independent Living System, United Health Centers of the San Joaquin Valley, PracticeMax, Lincare, Illuminate Education, Horizon Actuarial Services, Partnership HealthPlan of California, Bako Diagnostics, Rite Aid, Discovery Practice Management, 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 Defendants' failure to adequately protect Plaintiff and Class members' Personal and Medical Information.

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

47. Defendant requires its customers to provide PII "for business and compliance reasons." It collects, retains, and uses that data to maximize profits through predictive marketing and other targeted marketing practices. By collecting, using, and deriving significant benefit from customers' PII, Defendant had a legal duty to take reasonable steps to protect this information from disclosure. As discussed below, Defendants also had a legal duty to take reasonable steps to protect customers' PII under applicable federal and state statutes, including Section 5 of the Federal Trade

Commission Act ("FTC Act"), 15 U.S.C. § 45, and the California Consumer Protection Act of 2018 (the "CCPA"), Cal. Civ. Code § 1798, et seq. FTC Security Guidelines Concerning PII.

48. 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.

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

50. 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.

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

52. "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.

53. HIPAA's Security Rule requires Defendants 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.

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

55. HIPAA also required Defendants 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).

56. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendants 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***."[6]

57. The Federal Trade Commission ("FTC") has established security guidelines and recommendations to help entities protect PII and reduce the likelihood of data breaches. Defendants were 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).

58. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

59. In 2016, the FTC provided updated security guidelines in a publication titled Protecting Personal Information: A Guide for Business. Under these guidelines, companies should protect consumer information they keep; limit the sensitive consumer information they keep; encrypt sensitive information sent to third parties or stored on computer networks; identify and understand network vulnerabilities; regularly run up-to-date anti-malware programs; and pay

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

particular attention to the security of web applications – the software used to inform visitors to a company's website and to retrieve information from the visitors.

60. The FTC recommends that businesses do not maintain payment card information beyond the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

61. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

62. The FTC has brought several actions to enforce Section 5 of the FTC Act. According to its website:

> When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.

63. Defendant was aware or should have been aware of its obligations to protect its customers' PII and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers from unauthorized access. Among other violations, Defendant violated its obligations under Section 5 of the FTC Act.

64. For example, the length of time it took Defendant to inform Plaintiff and the Class about the Data Breach after Defendant discovered the incident indicates that it does not use an adequate intrusion detection system to immediately expose a data breach; does not sufficiently monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; does not properly monitor for the transmission of large amounts of data from the system;

and does not maintain an appropriate plan to respond effectively to a data breach in the event one occurs.

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

66. In addition to their obligations under federal and state laws, Defendants owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendants 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. Defendants owed a duty to Breach Victims to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the Personal and Medical Information of the Breach Victims.

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

68. Defendants owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendants 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.

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

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

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

72. Defendants owed a duty to Breach Victims whose Personal and Medical Information was entrusted to Defendants to disclose if their 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 Defendants.

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

74. Defendants 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 Defendants' Results in Debilitating Losses to Consumers

75. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[7] Cyber criminals can leverage Plaintiff 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.

[7] "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").

76. 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.

77. 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 Defendants 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.

78. This is not just speculative. As the FTC has reported, if hackers get access to Personal and Medical Information, they ***will*** use it.[8]

79. 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.[9]

80. 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.[10] 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.

81. 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

[8] 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.

[9] *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).

[10] *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/.

more "than identity thefts involving banking and finance, the government and the military, or education."[11]

82. "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."[12]

83. 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 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)]."[13] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[14]

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

85. 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.[15] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while

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

[12] *Id.*

[13] 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

[14] *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

[15] *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/.

nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[16]

86. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[17]

87. 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.

88. Defendants' offer of 24 months of free identity monitoring to Plaintiff and the Class is likewise insufficient. 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. In any case, 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.[18] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

89. 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.

---

[16] *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/.

[17] "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.

[18] *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.

90. 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;

e. Damages flowing from Defendants' 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.

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

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

V.

CLASS ACTION ALLEGATIONS

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

> All citizens of the State of California who provided their personal medical information to Defendants and/or their partner companies on or before February 21, 2024, and who received notices from Defendants that their information was compromised (hereinafter the "Class").

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

94. Plaintiff is informed and believes that the total number of Class Members exceeds millions of 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 at this time, such information can be ascertained through appropriate discovery, from records maintained by Defendants.

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

96. 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 Defendants failed to adequately safeguard Plaintiff's and the Class' Personal and Medical Information;

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

(c) Whether Defendants' 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, CCPA, UCL, and/or Defendant's other duties;

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

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

(g) Whether Defendants entered into implied contracts with Plaintiff and the members of the Class that included contract terms requiring Defendants to protect the confidentiality of Personal and Medical Information and have reasonable security measures;

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

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

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

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

(l) What equitable relief is appropriate to redress Defendants' wrongful conduct; and

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

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

97. Class Representative will fairly and adequately protect the interests of the Class. Moreover, Class Representative 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 has retained competent counsel experienced in class action litigation to further ensure such protection and intend to prosecute this action vigorously.

98. 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 Defendants 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 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.

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

100. Moreover, the Class members' individual damages are insufficient to justify the cost of litigation, so that in the absence of class treatment, Defendants' 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 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)

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

102. Defendant is a "provider of health care," within the meaning of Civil Code §56.05(m), a "contractor" within the meaning of Civil Code §56.05(d), a "recipient" under Civil Code §56.13, or an administrator under Civil Code §56.26, 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).

103. Plaintiff and the Class are "patients" within the meaning of Civil Code § 56.05(k). Furthermore, Plaintiff and the Class, as patients of Defendants, or their contracting entity, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), stored onto Defendants' server through their partner companies, on or before February 21, 2024.

104. On or about April 10, 2024, Defendants determined that the illegally accessed files involved Plaintiff's and the Class members' individual identifiable "medical information," within the meaning of Civil Code § 56.05(j),[19] including Plaintiff's and the Class members' "first name, last name, address, date of birth, health diagnosis, and/or medications and prescriptions."

105. Defendants were made aware of an unusual activity involving certain of their electronic files. Defendants immediately commenced an investigation to quickly assess the security of their systems. Through the investigation, Defendant determined that certain files were accessed and acquired on or about February 21, 2024 without authorization. During their investigation, Defendants determined that the information of certain individuals were present in the relevant files.

106. As a result of Defendants' 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.

107. 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).

//

//

[19] 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 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 server contained Plaintiff's and the Class members' names, dates of birth, and prescription information, and thus contained individually identifiable medical information as defined by Civil Code § 56.05(j)

SECOND CAUSE OF ACTION
(Violations of the CCPA, Cal. Civ. Code § 1798.150)
(Against All Defendants)

108. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

109. Plaintiff and the Class members hereby seek relief under § 1798.150(a), including, but not limited to, (i) recovery of actual damages or damages in an amount not less than $100 and not greater than $750 per consumer per incident, whichever is greater, (ii) injunctive or declaratory relief, and (iii) any other relief the Court deems proper, including attorneys' fees and costs pursuant to Cal. Code Civ. P. § 1021.5.

110. Plaintiff and Class members also seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continue to hold customers' PII, including Plaintiff's and Class members' PII. These individuals have an interest in ensuring that their PII is reasonably protected.

111. Defendant is a company organized or operated for the profit or financial benefit of its owners with annual gross revenues over $276.5 billion. Defendants collected consumers' PII as defined in Cal. Civ. Code § 1798.140.

112. Defendants violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and Class members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

113. Defendants collect consumers' personal information as defined in Cal. Civ. Code § 1798.140. Defendants have a duty to implement and maintain reasonable security procedures and practices to protect this personal information. As identified herein, Defendants failed to do so. As a direct and proximate result of Defendants' acts, Plaintiff's and Class members' personal information, including unencrypted names and birth dates, among other information, was subjected to unauthorized access and exfiltration, theft, or disclosure.

114. Plaintiff has served Defendant with a notice and opportunity to cure pursuant to Cal. Civ. Code §1798.150 by certified mail upon filing of this complaint.

115. Defendant has not responded to Plaintiff's Cal. Civ. Code §1798.150 letter. Specifically, Defendant failed to (i) provide an express written statement that the violations have been cured and that no further violations shall occur as required by § 1798.150; or (ii) "actually cure" its violation of Cal. Civ. Code §1798.150(a) within thirty days of Plaintiff's written notice of Defendants' violation of §1798.150(a). 84. Based on the foregoing, Plaintiff's claim for statutory damages under the CCPA is therefore proper.

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

116. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

117. Defendants engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, et seq.

118. Defendants engaged in unlawful acts and practices by maintaining sub-standard security practices and procedures as described herein, by soliciting, collecting, and profiting from Plaintiff's and Class members' PII knowing that it would not be adequately protected, and by storing Plaintiff's and Class members' PII in an unsecure electronic environment in violation of California's data breach statute, the CMIA and Cal. Civ. Code § 1798.81.5, which require Defendants to implement and maintain reasonable security procedures and practices to safeguard the PII of Plaintiff and the Class.

119. In addition, Defendants engaged in unlawful acts and practices by failing to disclose the Data Breach to the Plaintiff and the Class in a timely and accurate manner contrary to the duties imposed by Cal. Civ. Code §1798.82.

120. As alleged herein, Defendants engaged in negligence, among other unfair acts and practices. Plaintiff and Class members were directly and proximately harmed in several ways as a result of Defendants' unlawful and/or unfair conduct and are entitled to all available injunctive relief, including but not limited to an order mandating Defendants to (i) implement reasonable security measures to protect its customers' PII and (ii) provide prolonged free credit monitoring to customers affected by the Data Breach.

PRAYER FOR RELIEF

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

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

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

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

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

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

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

vii. Ordering that Defendants 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 Defendants to meaningfully educate their 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 Defendants 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 CCPA, Cal. Civ. Code § 1798.150 and 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: June 7, 2024 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: June 6, 2024 By: _____

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