SCHONBRUN SEPLOW HARRIS HOFFMAN & ZELDES, LLP
Helen I. Zeldes: SBN 220051
hzeldes@sshhzlaw.com
Ben Travis: SBN 305641
btravis@sshhzlaw.com
501 West Broadway, Suite 800
San Diego, CA 92101
Tel: (619) 400-4990

MIGLIACCIO & RATHOD LLP
Nicholas Migliaccio, *pro hac vice* anticipated
nmigliaccio@classlawdc.com
Jason Rathod, *pro hac vice* anticipated
jrathod@classlawdc.com
Selin Demir: SBN 331418
sdemir@classlawdc.com
412 H St NE
Washington, DC 20002
Tel: (202) 470-3520

Attorneys for Plaintiff and Proposed Class

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

MADELYN ROSEN, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

SCRIPPS HEALTH.,

Defendant.

CASE NO.: '21CV1358 JLS WVG

CLASS ACTION COMPLAINT

(1) Negligence;
(2) Breach of Implied Contract;
(3) Unjust Enrichment/Quasi-Contract;
(4) Violation of California Constitutional Right to Privacy, Cal. Const. art. I, § 1.,
(5) Violation of California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, et seq.,
(6) Violation of the California Unfair Competition Law, Cal. Bus. Prof. Code § 17200 *et seq*.,
(7) Violation of the California Customer Records Act, Civ. Code § 1798.82.

DEMAND FOR JURY TRIAL

Plaintiff Madelyn Rosen, individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against defendant Scripps Health ("Scripps" or "Defendant").

INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to exercise reasonable care in securing and safeguarding individual's sensitive personal data—including name, address, date of birth, health insurance information, medical record number, patient account number, and/or clinical information, such as physician name, date(s) of service, and/or treatment information (collectively known as "Private Information").

2. On May 1, 2021, Defendant first learned of "unusual network activity" whereby an unauthorized party accessed Defendant's systems housing personal information (the "Security Breach"). As a result, the Private Information of thousands of patients was compromised.

3. Defendant did not formally send patients a breach notification letter for one month. However, for Plaintiff and those similarly situated, many patients were notified of the breach through disruption in healthcare services.

4. On or about May 10, 2021, Defendant announced that, it was discovered that Patient Private Information had been compromised during the breach than previously thought, with additional patients having been affected.

5. Defendant's security failures enabled the hackers to steal the Private Information of Plaintiff and members of the Class (defined below). These failures put Plaintiff' and Class members' Private Information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiff and Class members associated with delayed healthcare treatment, time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Security Breach, including, as appropriate, reviewing records for fraudulent charges and healthcare services billed for but not received, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, and the stress, nuisance and

annoyance of dealing with all issues resulting from the Security Breach.

6. The Security Breach was caused and enabled by Defendant's violation of its obligations to abide by best practices and industry standards concerning the security of patients records and Private information. Defendant failed to comply with security standards and allowed their customers' Private Information to be compromised by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

7. Accordingly, Plaintiff asserts claims for violations of negligence, breach of implied contract, unjust enrichment/quasi-contract, the California Constitution's right to privacy (Cal. Const., art. I, § 1), California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, et seq., and California's Unfair Competition Law ("UCL"), Cal. Bus. Prof. Code § 17200, et seq., and seek injunctive relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

PARTIES

Plaintiff

8. Plaintiff and the other Class members have suffered actual injury and at risk of further imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their Private Information being stolen in the Security Breach.

9. The injuries suffered by Plaintiff and Class members as a direct result of the Security Breach include one or more of the following:

a. unauthorized use of their Private Information;

b. theft of their Private Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their Private Information;

e. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of

the Security Breach, including reviewing records for fraudulent charges and healthcare services billed for but not received, attempting to receive medical information, paying for credit monitoring services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Security Breach; and

f. the loss of Plaintiff' and Class members' privacy.

Plaintiff Madelyn Rosen

10. **Plaintiff Madelyn Rosen** is a resident of California. Rosen has routinely received medical care from providers in Defendant's network, leading to her Private Information being exposed as a result of Defendant's inadequate security. Rosen received an informal notification of the data breach when she was unable to get a report from her radiology appointment. Attempting to get her health information from Defendant, Rosen called multiple times, and was unable to reach anybody. Defendant could only share an image, with no report. Rosen estimates both her and her doctor lost about 24 hours attempting to receive her health report from Defendant while Defendant was responding to the Security Breach. Rosen is fearful of the risk of her exposed data, and now must commit future time to checking her Medicare reports for fraudulent charges. Rosen is a professional insurance agent, and she is aware that few people check their Medicare reports to see what charges come through, which creates waste and fraud. Rosen has been a patient at neighboring hospitals and has never received a breach notification from any of them.

Defendant

11. Defendant Scripps Health is a California not-for-profit corporation which operates a group of $3.1 billion nonprofit hospitals and healthcare providers in the Southern California region.

12. Scripps is headquartered at 10140 Campus Point Drive, San Diego, California 92121.

JURISDICTION AND VENUE

13. The Court has jurisdiction over Plaintiff' claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

14. The Court has personal jurisdiction over Defendant because its principal place of business is located, and they conduct substantial business, in this District.

15. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore reside in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

FACTUAL ALLEGATIONS

16. Defendant provides healthcare services to thousands of patients per year in California. As part of its business, Defendant stores a vast amount of its patients' Private Information. In doing so, Defendant was entrusted with, and obligated to safeguard and protect, the Private Information of Plaintiff and the Class in accordance with all applicable laws.

17. In April 2021, Defendant first learned of "unusual network activity" whereby an unauthorized party may have gained access to the emails and attachments of several of Defendant's employee email accounts that may have contained patients' Private Information including "name, dates of birth, health insurance information, medical record number, patient account number, and/or clinical information such as physician name, date(s) of service, and/or treatment information."

18. Upon learning of the Security Breach, Defendant's medical operations hit a standstill. Defendant reviewed the unusual network activity, but did not provide reconciliation to Plaintiff or Class members before and after sending the breach notification. As a result of the Security Breach, Private Information was stolen from over 147,267 patients between April 2021 and June 2021.

19. On June 1, 2021, Defendant formally announced its data breach to the California State Attorney General's office.

20. In a notice mailed to Plaintiff by Defendant in June 2021, Defendant stated:

> [W]e recommend that you review the statements you receive from your healthcare providers and health insurer. If you see any medical services that you did not receive, please call the provider or insurer immediately. To help prevent something like this from happening again, we are continuing to implement enhancements to our information security, systems, and monitoring capabilities.

21. Defendant has yet to affirmatively notify impacted patients individually regarding which specific data of theirs were stolen.

22. The Breach occurred because Defendant failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated public warnings to the healthcare industry about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other healthcare providers. For example, Defendant failed to maintain basic security measures. Defendant failed to disclose to Plaintiff and Class members the material fact that it did not have adequate data security practices to safeguard customers' personal data, and in fact falsely represented that their security measures were sufficient to protect the Personal Information in its possession.

23. Defendant's failure to provide immediate formal notice of the Breach to Plaintiff and Class members exacerbated the injuries resulting from the Breach.

A. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Patients' Private Information Despite Having Resources

24. Defendant is one of San Diego's largest health systems, as a $3.1 billion non-profit with 15,000 employees. Defendant gained $106 million in the past year. Yet Defendant did not allocate adequate resources for cybersecurity protection of patient information.

25. Under the Health Insurance Portability Act of 1996 ("HIPPA") Defendant had a heightened duty to protect patient Private Information.

26. After Defendant experienced the data breach, the entire Scripps Health system came to a standstill, unable to function or provide basic medical services and administration. Defendant had to turn away patients to other healthcare providers. [1] Patients could not schedule or reach medical staff for questions necessary to obtain healthcare. Patients already invested in Scripps Health struggled to obtain healthcare from Scripps, and options to immediately switch to nearby healthcare providers were limited due to the major bureaucratic struggle and cost that comes with transferring patient Private Information. Due to Scripps's size and market dominance in the San Diego area the burden to transfer patient Private Information in order to access healthcare elsewhere felt troublesome. So troublesome, that not obtaining necessary healthcare for the time period felt like a better option.

27. Defendant advertises, "At Scripps we are committed to protecting the privacy of your health information." Defendant's website continued to advertise this message even one month after notifying thousands of patients that Defendant exposed patient Private Information.

28. Defendant failed to ensure that proper data security safeguards were being implemented throughout the breach period.

29. Defendant failed to ensure its healthcare operations would not be impacted in case of a data breach.

30. Defendant had obligations created by HIPAA, industry standards, common law, and representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

31. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligations to keep such information confidential and secure from unauthorized access.

[1] https://www.sandiegouniontribune.com/news/health/story/2021-05-05/state-regulator-watching-scripps-ransomware-attack-closely

32. Prior to and during the Security Breach, Defendant promised patients that their Private Information would be kept confidential, through its Notice of Privacy Practices. [2] For example, "We understand that information about you and your health is confidential. We are committed to protecting the privacy of this information."

33. Defendant's failure to provide adequate security measures to safeguard patients' Private Information is especially egregious because Defendant operate in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to patients' highly confidential Private Information.

34. Ponemon Institute, an expert in the annual state of cybersecurity, had indicated that in 2020 healthcare institutions were the top target for cyber-attacks.

35. In fact, Defendant has been on notice for years that the medical industry is a prime target for scammers because of the amount of confidential patient information maintained. In 2019 alone, numerous entities in the healthcare sector suffered high-profile data breaches including Quest Diagnostics and LabCorp.

36. Defendant had resources for years to address their data security. In 2016, Scripps was named one of the area's largest healthcare providers. In 2018, Defendant's President and CEO advocated for making "market share play" to obtain greater market share. [3] Defendant has managed to make themselves one of the only major healthcare providers in the San Diego area, leaving few options for patients who may not want to share their Private Information with Scripps. Because of Scripps market dominance, patients feel obligated to provide Private Information to Scripps in order to receive local healthcare.

B. Defendant's Data Security Failures and HIPAA Violations

37. Defendant's data security lapses demonstrate that failed to honor their duties and promised by not:

---

[2] https://www.scripps.org/sparkle-assets/documents/100-8560-217sw-english.pdf

[3] https://www.scripps.org/news_items/6449-scripps-ceo-discusses-market-trends-in-current-health-care-environment

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting patients' Private Information;

c. Properly monitoring their own data security systems for existing intrusions;

d. Ensuring that they employed reasonable data security procedures;

38. Ensuring the confidentiality and integrity of electronic protected health information ("PHI") they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

40. Implementing policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

41. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

42. Protecting against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

43. Protecting against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

44. Ensuring compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or

45. Training all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b).

C. Damages to Plaintiff and the Class

46. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Security Breach.

47. Plaintiff and the Class have experienced or currently face a substantial risk of out-of-pocket fraud losses such as, e.g., credit cards opened in their name, medical services billed in their name, suspicious phones calls, Medicare fraud, and similar identity theft.

48. Class members may also incur out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Security Breach. Plaintiff here feels obliged to continue purchasing credit monitoring out of pocket in response to being notified of the Security Breach. Defendant offered no complimentary credit monitoring to mitigate the harm they caused.

49. Plaintiff and Class members suffered a "loss of value" of their Private Information when it was acquired by cyber thieves in the Security Breach. Numerous courts have recognized the propriety of "loss of value" damages in data breach cases.

50. Class members who paid Defendant for their services were also damaged via "benefit of the bargain" damages. Such members of the Class overpaid for a service that was intended to be accompanied by adequate data security, but was not. Part of the price Class members paid to Defendant was intended to be used by Defendant to fund adequate data security. Defendant did not properly comply with their data security obligations. Thus, the Class members did not get what they paid for.

51. Members of the Class have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

52. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit accounts were the most common types of misused information. [4]

---

[4] *See* DOJ, *Victims of Identity Theft, 2014* at 1 (Nov. 13, 2017), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf.

53. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. [5]

54. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the medical context, Private Information can be used to submit false insurance claims, obtain prescription drugs or medical devices for black-market resale, or get medical treatment in the victim's name. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit and tax filings for an indefinite duration.

55. Medical information is especially valuable to identity thieves. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

COMMON FACTUAL ALLEGATIONS

D. The Value of Privacy Protections and Private Information

56. The fact that Plaintiff' and Class members' Private Information was stolen—and might presently be offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

---

[5] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number[.]" *Id.*

57. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third-party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information. [6]

58. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States. [7]

59. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[8]

60. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information. [9] The idea is to

---

[6] Tr. at 8:2-8, Federal Trade Commission, *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data* (Mar. 13, 2001) available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[7] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

[8] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[9] *Web's Hot New Commodity: Privacy*, *supra* note 7.

give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

61. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349. [10]

62. The value of Plaintiff and Class members' Private Information on the black market is substantial, ranging, for example, from $1.50 to $90 per payment card number. [11]

63. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the medical industry.

64. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented intrusion into their systems and, ultimately, the theft of their patients' Private Information.

65. Given these facts, any company that transacts business with patients and then compromises the privacy of patients' Private Information has thus deprived patients of the full monetary value of their transaction with the company.

---

[10] *See* DOJ, *Victims of Identity Theft, 2014*, *supra* note 3, at 6.

[11] Leapfrog, *The Cyber Black Market: What's Your Bank Login Worth* (Mar. 1, 2011), available at https://leapfrogservices.com/the-cyber-black-market-whats-your-bank-login-worth/.

CLASS ACTION ALLEGATIONS

66. Plaintiff brings all counts, as set forth below, individually and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a **Nationwide Class** defined as:

> All persons who submitted their Private Information to Defendant or Defendant's affiliates and whose Private Information was compromised as a result of the data breach discovered in or about April 2021 (the "Nationwide Class").

67. In addition to and/or in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of the following **California Subclass**:

> All residents of California who submitted their Private Information to Defendant or Defendant's affiliates and whose Private Information was compromised as a result of the data breach discovered in or about April 2021 (the "California Subclass," collectively with the Nationwide Class, the "Class").

68. Excluded from both the Nationwide Class and the California Subclass are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

69. Certification of Plaintiffs claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

70. **Numerosity**—Federal Rule of Civil Procedure 23(a)(1). The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class and Subclass both number in the tens of thousands.

71. **Commonality and Predominance**—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3). Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, inter alia:

a. Whether Defendant's data security systems prior to and during the

Security Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

b. Whether Defendant's data security systems prior to and during the Security Breach were consistent with industry standards;

c. Whether Defendant properly implemented their purported security measures to protect Plaintiff and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendant took reasonable measures to determine the extent of the Security Breach after they first learned of same;

e. Whether Defendant disclosed Plaintiff and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendant's conduct constitutes breach of an implied contract;

g. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff and the Class's Private Information;

h. Whether Defendant were negligent in failing to properly secure and protect Plaintiff and the Class's Private Information;

i. Whether Defendant was unjustly enriched by its actions; and

j. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

72. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

73. **Typicality**—Federal Rule of Civil Procedure 23(a)(3). Plaintiff's claims are

typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

74. **Adequacy of Representation**—Federal Rule of Civil Procedure 23(a)(4). Plaintiff is an adequate representative of the Nationwide Class and the Subclass because her interests do not conflict with the interests of the Classes she seeks to represent, she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and her counsel.

75. **Injunctive Relief-**-Federal Rule of Civil Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

76. **Superiority**—Federal Rule of Civil Procedure 23(b)(3). A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

77. Nexus to California: The State of California has a special interest in regulating the affairs of corporations that do business here and persons who live here. Defendant is based in San Diego, California. Defendant performed the unlawful and deceptive conduct described in

this Complaint from its headquarters in the San Diego Area. Additionally, Defendant has more patients in California than in any other state. Accordingly, there is a substantial nexus between Defendant's unlawful behavior and California such that the California courts should take cognizance of this action on behalf of a class of individuals who reside in California and the United States

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Subclass)

78. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

79. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in their computer systems and on their networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

80. Defendant owed a duty of care not to subject Plaintiff'and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

81. Defendant owed numerous duties to Plaintiff and the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;

b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

82. Defendant also breached their duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

83. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the medical industry.

84. Defendant knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff and Class members' Private Information.

85. Defendant breached their duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class members' Private Information.

86. Because Defendant knew that a breach of their systems would damage thousands of their customers, including Plaintiff and Class members, Defendant had a duty to adequately protect their data systems and the Private Information contained thereon.

87. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

88. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all

of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

89. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

90. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential Private Information.

91. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff' and Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

92. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Security Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

b. Failing to adequately monitor the security of Defendant's networks and systems;

c. Allowing unauthorized access to Class members' Private Information;

d. Failing to detect in a timely manner that Class members' Private Information had been compromised; and

e. Failing to timely notify Class members about the Security Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

93. Through Defendant's acts and omissions described in this Complaint, including their failure to provide adequate security and their failure to protect Plaintiff and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff and Class members' Private Information during the time it was within Defendant's possession or control.

94. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

95. Neither Plaintiff nor the other Class members contributed to the Security Breach and subsequent misuse of their Private Information as described in this Complaint.

96. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

97. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Subclass)

98. Plaintiff fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

99. Defendant solicited and invited Class members to provide their Private Information as part of Defendant's regular business practices. When Plaintiff and Class members made and paid for purchases of Defendant's services and products, they provided their Private Information to Defendant.

100. In so doing, Plaintiff and Class members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely detect any breaches of their Private Information. In entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

101. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

102. Plaintiff and Class members would not have provided and entrusted their Private Information with Defendant in the absence of the implied contract between them and Defendant.

103. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

104. Defendant breached the implied contracts they made with Plaintiff and Class members by failing to safeguard and protect their Private Information and by failing to timely detect the data breach within a reasonable time.

105. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant, Plaintiff and Class members, Plaintiff and Class members sustained actual losses and damages as described in detail above.

106. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free lifetime credit monitoring to all Class members.

COUNT III
UNJUST ENRICHMENT/QUASI-CONTRACT
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Subclass)

107. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

108. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their Private Information. In exchange, Plaintiff and Class members should have received from Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their Private Information with adequate data security.

109. Defendant knew that Plaintiff and Class members conferred a benefit on them and accepted and has accepted or retained that benefit. Defendant profited from Plaintiff's purchases and used Plaintiff's and Class members' Private Information for business purposes.

110. Defendant failed to secure Plaintiff and Class members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiff and Class members' Private Information provided.

111. Defendant acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

112. If Plaintiff and Class members knew that Defendant would not secure their Private Information using adequate security, they would not have made purchases at Defendant's stores.

113. Plaintiff and Class members have no adequate remedy at law.

114. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred on them.

115. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid.

//

//

COUNT IV
VIOLATION OF THE CALIFORNIA CONSTITUTION'S RIGHT TO PRIVACY
(Cal. Const., art. I, § 1)
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Subclass)

116. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

117. The California Constitution provides:

> "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possession, and protecting property, and pursuing and obtaining safety, happiness, and privacy." (Cal. Const., art. I. § 1.)

118. Plaintiff and the Class have a legally recognized and protected privacy interest in the personal and financial information provided to and obtained by Defendant, including but not limited to an interest in precluding the dissemination or misuse of this sensitive and confidential information and the misuse of this information for malicious purposes such as theft of funds.

119. Plaintiff and the Class reasonably expected Defendant would prevent the unauthorized viewing, use, manipulation, exfiltration, theft, and disclosure of their personal and financial information and the unauthorized use of their Private Information.

120. Defendant's conduct described herein resulted in a serious invasion of privacy of Plaintiff and the Class, as the release of Private Information could highly offend a reasonable individual.

As a direct consequence of the actions as identified above, Plaintiff and the Class members suffered harms and losses including but not limited to economic loss, the loss of control over use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation and attempt to cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal and financial information disclosed.

COUNT V
VIOLATION OF CALIFORNIA'S CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA")
CAL. CIV. CODE § 56, et seq.
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the Subclass)

121. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

122. Defendant is a "provider of healthcare," as defined in Cal. Civ. Code § 56.06, and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

123. Defendant is licensed under California under California's Business and Professions Code, Division 2. See Cal. Bus. Prof. Code § 4000, et seq. and therefore qualifies as a "provider of healthcare" under the CMIA.

124. Plaintiff and the Class are "patients," as defined in CMIA, Cal. Civ. Code § 56.05(k) ("'Patient' means any natural person, whether or not still living, who received healthcare services from a provider of healthcare and to whom medical information pertains.").

125. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Security Breach resulted from the inactions of Defendant, including its failure to adequately implement sufficient data security measures and protocols to protect Plaintiff and Class members' Personal and Medical Information, which allowed hackers to obtain Plaintiff and the Class members' medical information.

126. Defendant's negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff and the Class to unauthorized persons and the breach of the confidentiality of that information. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff and Class members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

127. Defendant's systems and protocols did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A).

128. Plaintiff and the Class were injured and have suffered damages, as described above, from Defendant's illegal disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees, expenses and costs.

COUNT VI
CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL"),
Cal. Bus. Prof. Code § 17200, et seq.,
(On Behalf of all Plaintiff and the Nationwide Class or, alternatively, by Plaintiff on behalf of the Subclass)

129. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

130. 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 Plaintiff and Class member's Personal and Medical Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that Defendant would and did comply with the requirement of relevant federal and state laws relating to privacy and security of Plaintiff and Class's Private Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Private Information;

b. By soliciting and collecting Private Information from Plaintiff and Class members without adequately protecting or storing Private Information;

c. By violating the privacy and security of HIPPA, 42 U.S.C. §1302d, et seq.; and

d. by violating the CMIA, Cal. Civ. Code § 56, et seq.

131. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities that 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., and the CMIA, Cal. Civ. Code § 56, et seq.

132. 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 delayed healthcare treatment, overpayments Defendant received to maintain adequate security measures and 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.

133. Defendant knew or should have known that its computer systems were vulnerable and thus inadequate to safeguard Plaintiff and Class members' Private Information and that the risk of a data breach or theft was highly likely. Defendant should have prepared for how to continuously provide healthcare treatment in case of a Security Breach. Defendant had resources to secure and/or prepare for protecting patient Private Information in a Security Breach. 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.

134. 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.

COUNT VII
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT ("CRA"), Cal. Bus. Prof. Code § 17200, et seq., (On Behalf of all Plaintiff and the Nationwide Class or, alternatively, by Plaintiff on behalf of the Subclass)

135. Plaintiff realleges and incorporates the above allegations by reference as if set forth fully herein.

136. At all relevant times, Defendant was a "business" under the terms of the CRA as a non-profit operating in the State of California that owned or licensed computerized data that included the personal information of Plaintiff and the Class.

137. At all relevant times, Plaintiff and the Class were "customers" under the terms of the CRA as natural persons who provided personal information to Defendant for the purpose of purchasing or leasing a product or obtaining a service from Defendant

138. Section 1798.82 requires that disclosure "shall be made in the most expedient time possible and without unreasonable delay…." By the acts described above, Defendant violated the CRA by allowing unauthorized access to customers' personal and financial information and then failing to inform them, for weeks, when the unauthorized use occurred, thereby failing in its duty to inform its customers of unauthorized access expeditiously and without unreasonable delay.

139. The Security Breach described herein is a "breach of the security system" under Section 1798.82.

140. As a direct consequence of the actions as identified above, Plaintiff and the Class incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and/or cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal and financial information disclosed, that they would have not otherwise lost had Defendant immediately informed them of the unauthorized use.

141. Plaintiff accordingly requests the Court enter an injunction requiring Defendant to implement and maintain reasonable security procedures, including, but not limited to: (1) order Defendant to utilize stronger industry standard data security measures and file transfer software for the transfer and storage of customer data; (2) order Defendant to engage third party security auditors and/or penetration testers on a regular basis as well as internal security to conduct testing inclusive of simulated attacks and institution-wide personnel training; (3) order

Defendant to create training and protocol to give patients and customers seamless access to medical care, scheduling, and reasonable access to the hospital despite future interruption of its computer systems; (4) order Defendant, consistent with industry standard practices, to periodically conduct internal training and education to inform internal personnel how to identify and contain a breach when it occurs, and how to respond to a breach; and (5) order Defendant to meaningfully educate its customers and patients about threats they face as a result of losing their Private Information to unauthorized third parties.

142. Plaintiff further requests the Court require Defendant to identify all of its impacted clients, to what degree their information was stolen, and to notify all members of the Class who have not yet been informed of the Data Breach by written email within 24 hours of discovery of a breach, possible breach, and by mail within 72 hours.

143. As a result of Defendant's violations, Plaintiff and the Class are entitled to all actual and compensatory damages according to proof, to non-economic injunctive relief allowable under the CRA, and to such other and further relief as this Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a. For an order certifying the proposed classes and appointing Plaintiff and her counsel to represent the classes;

b. For an order awarding Plaintiff and Class members actual, statutory, punitive, and/or any other form of damages provided by and pursuant to the statutes cited above;

c. For an order awarding Plaintiff and Class members restitution, disgorgement and/or other equitable relief provided by and pursuant to the statutes cited above or as the Court deems proper;

d. For an order or orders requiring Defendant to adequately remediate the Breach and its effects.

e. For an order awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

f. For an order awarding Plaintiff and Class members treble damages, other enhanced damages and attorneys' fees as provided for under the statutes cited above and related statutes;

g. For an order awarding Plaintiff and the Class members reasonable attorneys' fees and costs of suit, including expert witness fees;

h. For an order awarding such other and further relief as this Court may deem just and proper.

Dated: July 28, 2021

SCHONBRUN SEPLOW HARRIS HOFFMAN & ZELDES, LLP

By: */s/ Helen I. Zeldes*
Helen I. Zeldes
Ben Travis

MIGLIACCIO & RATHOD LLP
Selin Demir, Esq. SBN 331418
Nicholas A. Migliaccio, Esq.*
Jason S. Rathod, Esq.*
412 H Street N.E., Ste. 302
Washington, DC 20002
Tel: (202) 470-3520
* *pro hac vice* forthcoming

Attorneys for Plaintiff.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims so triable.

Dated: July 28, 2021

SCHONBRUN SEPLOW HARRIS HOFFMAN & ZELDES, LLP

By: */s/ Helen I. Zeldes*
Helen I. Zeldes
Ben Travis

MIGLIACCIO & RATHOD LLP
Selin Demir, Esq. SBN 331418
Nicholas A. Migliaccio, Esq.*
Jason S. Rathod, Esq.*
412 H Street N.E., Ste. 302
Washington, DC 20002
Tel: (202) 470-3520
* *pro hac vice* forthcoming

Attorneys for Plaintiff and the Proposed Class.