Jason S. Hartley (SBN 192514)
HARTLEY LLP
101 West Broadway, Suite 820
San Diego, California 92101
Tel: 619-400-5822
hartley@hartleyllp.com

Norman E. Siegel
J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel: 816-714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

DENISE MENEZES, individually and on behalf of all others similarly situated,

Plaintiff,

v.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA d/b/a UC SAN DIEGO HEALTH,

Defendant.

Case No. **'21CV1641 BEN JLB**

CLASS ACTION COMPLAINT

(1) Violation of the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.150
(2) Violation of California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq*.
(3) Violation of California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(4) Negligence
(5) Negligence *Per Se*
(6) Breach of Contract
(7) Breach of Implied Contract
(8) Unjust Enrichment/Quasi Contract
(9) Breach of Confidence
(10) Declaratory Relief

DEMAND FOR JURY TRIAL

Plaintiff Denise Menezes ("Plaintiff"), by and through the undersigned counsel, brings this class action complaint against Defendant the Regents of The University of California d/b/a UC San Diego Health ("Defendant" or "UC San Diego Health"), on behalf of herself and all others similarly situated. Plaintiff makes the following allegations based upon personal knowledge as to her own actions and upon information and belief as to all other matters.

NATURE OF THE ACTION

1. On July 27, 2021, UC San Diego Health, the academic health system of the University of California, San Diego, published a notice on its website stating that it was subject of a data breach whereby hackers gained unauthorized access to employees' email accounts for more than four months between December 2, 2020 and April 8, 2021 (the "Data Breach"). The hackers were able to access and exfiltrate highly-sensitive information stored on UC San Diego Health's servers, including patients' full names, addresses, dates of birth, email addresses, fax numbers, claims information (dates and cost of health care services and claims identifiers), laboratory results, medical diagnosis and conditions, Medical Record Numbers and other medical identifiers, prescription information, treatment information, medical information, Social Security numbers, government identification numbers, payment card numbers and financial account numbers and security codes, student ID numbers, and usernames and passwords ("PII").

2. The Data Breach occurred because UC San Diego Health failed to implement reasonable security procedures and practices, failed to provide its employees with basic cybersecurity training designed to prevent "phishing" attacks, failed to take adequate steps to monitor for and detect unusual activity on its servers, failed to disclose material facts surrounding its deficient data security protocols, and failed to timely notify the victims of the Data Breach.

3. As a result of UC San Diego Health's failure to protect the sensitive information it was entrusted to safeguard, Plaintiff and class members did not

receive the benefit of their bargain with UC San Diego Health and now face a significant risk of medical-related identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

PARTIES

4. Plaintiff Denise Menezes is a resident of El Cajon, California and healthcare patient of Moores Cancer Center, a member facility of UC San Diego Health.

5. Defendant the Regents of the University of California is a corporation established under the Constitution of the State of California to manage, operate, and administer the University of California as a public trust. Under the pseudonym "UC San Diego Health System," the Regents of the University of California provides regional administration of various medical facilities, including medical centers, clinics, express and urgent care locations, academic health centers, health professional schools, and regional supporting services. Defendant is doing business in multiple locations throughout San Diego County. The UC San Diego Health System, and its member medical facilities, are operated at least in part for the profit or financial benefit of the Regents of the University of California.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332, the Class Action Fairness Act, because: (i) there are 100 or more class members; (ii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs; and (iii) there is minimal diversity because members of the Class are citizens of different states from Defendant.

7. This Court has personal jurisdiction over Defendant because it operates in this District and intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

8. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because significant events giving risk to this case took place in this District, and because

Defendant is authorized to conduct business in this District, has intentionally availed itself of the laws and markets within this District, does substantial business in this District, and is subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

UC San Diego Health's Privacy Practices

9. UC San Diego Health is the academic health system of the University of California, San Diego, and is comprised of a number of health institutions located in the San Diego region, including UC San Diego Medical Center, Jacobs Medical Center, Sulpizio Cardiovascular Center, Shiley Eye Institute, Moores Cancer Center, and Koman Family Outpatient. UC San Diego Health is one of the largest revenue drivers for the Regents of the University of California, demonstrated by the fact that UC San Diego Health CEO Patricia Maysent earned more than $1.1 million in gross compensation in 2020.

10. In the course of providing medical services at these institutions, UC San Diego Health requires patients to provide personal information including their full names, home addresses, dates of birth, email addresses, and Social Security numbers, financial information such as bank account and payment card numbers, and medical information including medical histories, past treatment records, prescription information, health provider information, and health insurance coverage. As a result, when patients are treated by a UC San Diego Health-affiliated institution, their highly sensitive PII is stored on centralized servers maintained by UC San Diego Health.

11. Given the amount and sensitive nature of the data it collects, UC San Diego Health maintains a "Notice of Privacy Practices" which describes how medical information about its patients will be used and disclosed.[1] UC San Diego Health represents that "All new patients are provided a copy of the Notice of

[1] https://health.ucsd.edu/hipaa/Pages/hipaa.aspx (last visited September 20, 2021).

Privacy Practices and will be asked to sign a form indicating they have read and reviewed this notice."[2]

12. The Notice of Privacy Practices states that "UC San Diego Health is committed to protecting the privacy of your medical or health information. We are required by law to maintain the privacy of your health information. We will follow the legal duties and privacy practices described in this notice."[3] Those duties include "the right to be notified if we discover a breach that may have compromised the privacy or security of your information" and that UC San Diego Health will not "share and use your health information" in ways "not covered by this Notice" without written authorization.[4]

13. UC San Diego Health further represents that "UC San Diego Health has always had privacy and patient confidentiality standards in place to limit unauthorized access or disclosure to personal health information[.]"[5] In a separate notice entitled "Patient Rights and Responsibilities", UC San Diego Health represents that all patients have a right to "[c]onfidential treatment of all communications and records pertaining to your care and stay in the hospital."[6]

The Data Breach

14. Contrary to its representations, on December 2, 2020, hackers were able to access the email accounts of UC San Diego Health's employees through a successful "phishing" attempt. Phishing is the practice of sending fraudulent emails, oftentimes targeting a company's employees, purporting to be from a reputable

---

[2] https://health.ucsd.edu/patients/yourhospitalstay/Pages/patientrights.aspx (last visited September 20, 2021).

[3] https://health.ucsd.edu/hipaa/Pages/hipaa.aspx (last visited September 20, 2021).

[4] *Id*.

[5] https://health.ucsd.edu/patients/yourhospitalstay/Pages/patientrights.aspx (last visited September 20, 2021).

[6] https://health.ucsd.edu/patients/yourhospitalstay/Documents/Patient%20Rights%20and%20Responsibilities%20Handout.pdf (last visited September 20, 2021).

source in order to induce the employee to reveal sensitive information or to deploy malicious software on the company's network.

15. After gaining access, the hackers were able to maneuver unimpeded through UC San Diego Health's servers for months as the organization had inadequate controls in place to monitor for unusual and irregular activity. Even when unusual activity was first discovered on March 12, 2021, it took UC San Diego Health several more weeks until April 8, 2021 to actually terminate the unauthorized access. Consequently, during a period of more than four months, hackers had unfettered access to troves of unencrypted information stored on UC San Diego Health's servers, including patients' financial, medical, and treatment information.

16. Following the Data Breach, UC San Diego Health did not disclose what happened until July 27, when it posted a notice on its website regarding the Data Breach. Of course, a website posting did not identify which specific patients were impacted and was inadequate to affirmatively alert individuals impacted by the Data Breach to take measures to protect themselves. Inexplicably, UC San Diego Health waited until September 9, 2021, to begin individually notifying patients whose PII was exposed in the Data Breach.

The Data Breach was Preventable

17. Following the Data Breach, UC San Diego Health stated that it "enhanced our security controls" in order to prevent something like this from happening again.[7] In particular, UC San Diego Health stated that it "began taking remediation measures which have included, among other steps, changing employee credentials, disabling access points, and enhancing security processes and procedures."[8] But the "enhancements" undertaken by UC San Diego Health are

[7] https://health.ucsd.edu/data-security/Pages/default.aspx (last visited September 20, 2021).

[8] *Id.*

industry-standard measures that should have been implemented long before the Data Breach occurred. This is especially true given that the healthcare industry is frequently one of the most targeted sectors for cyberattacks and that phishing attacks have increased precipitously over the last several years.

18. Healthcare providers like UC San Diego Health are prime targets because of the information they collect and store, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and personal information of employees and patients—all extremely valuable on underground markets.

19. This was known and obvious to UC San Diego Health as it observed frequent public announcements of data breaches affecting healthcare providers and knew that information of the type it collected, maintained, and stored is highly coveted and a frequent target of hackers. In fact, UC San Diego Health has previously been the subject of data security incidents that should have put in on high alert that it was a prime target for cyberattacks.

20. For example, in September 2016, the UC San Diego School of Medicine notified individuals that an electronic file containing the first and last names of school of medicine trainees, their social security numbers, and an internal UC San Diego index number was accessible on the internet for anyone to access. The school offered credit monitoring for affected individuals.[9]

21. In December 2017, UC San Diego Health learned that an unauthorized third party gained access to one of its business associates' medical transcription platforms containing names, dates of birth, ages, genders, medical record numbers, and clinical information for a number of patients. Well over six months later, UC San Diego Health informed affected individuals of the breach, noting that "[o]ne of

[9] https://oag.ca.gov/system/files/Final%20GME%20Notice%20Letter_0.pdf (last visited September 20, 2021).

UC San Diego Health's top priorities is to protect and maintain the confidentiality of patient information."[10]

22. According to a report by the HIPAA Journal, "data breach statistics clearly show there has been an upward trend in data breaches over the past 10 years, with 2020 seeing more data breaches reported than any other year since records first started being published."[11] In fact, healthcare data breaches were up 55% in 2020 from the prior year alone.[12]

23. Phishing attacks in particular have been on the rise. According to the Federal Bureau of Investigation (FBI), phishing was the most common type of cybercrime in 2020 and phishing incidents nearly doubled in frequency between 2019 and 2020.[13] According to Verizon's 2021 Data Breach Investigations Report (DBIR), phishing is the top "action variety" seen in breaches in the last year and 43% of breaches involved phishing and/or pretexting.[14]

24. The risk is so prevalent for healthcare providers that on October 28, 2020, the Federal Bureau of Investigation (FBI) and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[15] The Cybersecurity and Infrastructure Security Agency (CISA), the

---

[10] https://oag.ca.gov/system/files/ACID_PRINTERPROOFS_ACID_20180627_UCSD501_R1_1.pdf (last visited September 20, 2021).

[11] https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited September 20, 2021).

[12] https://www.cpomagazine.com/cyber-security/healthcare-cyber-attacks-rise-by-55-over-26-million-in-the-u-s-impacted/ (last visited September 20, 2021).

[13] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited September 20, 2021).

[14] https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited September 20, 2021).

[15] https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited September 20, 2021).

Department of Health and Human Services (HHS), and the FBI issued the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[16]

25. It is well known that use of stolen credentials through "phishing" scams have long been the most popular and effective method of gaining authorized access to a company's internal networks and that companies should activate defenses to prevent such attacks.

26. There are two primary defenses to "phishing" scams: employee education and technical security barriers. Employee education is the process of making employees aware of common spoofing scams and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. For example, a common phishing e-mail is an "urgent" request from a company "executive" requesting confidential information in an accelerated timeframe. The request may come from an e-mail address that appears official but contains only one different number or letter. Other phishing methods include baiting a user to click a malicious link that redirects them to a nefarious website or to download an attachment containing malware.

27. Employee education provides the easiest method to assist employees in properly identifying fraudulent e-mails and prevent unauthorized access of sensitive internal information. According to September 2020 guidance from CISA, organizations housing sensitive data should "[i]mplement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity" and conduct "organization-wide phishing tests to gauge user

[16] *Id.*

awareness and reinforce the importance of identifying potentially malicious emails."[17]

28. From a technical perspective, companies can also greatly reduce the flow of phishing e-mails by installing software that scans all incoming messages for harmful attachments or malicious content and implementing certain security measures governing e-mail transmissions, including Sender Policy Framework (SPF) (e-mail authentication method used to prevent spammers from sending messages on behalf of a company's domain), DomainKeys Identified Mail (DKIM) (e-mail authentication method used to ensure messages are not altered in transit between the sending and recipient servers), and Domain-based Message Authentication, Reporting and Conformance (DMARC), which "builds on the widely deployed [SPF] and [DKIM] protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email."[18]

29. Additionally, because the goal of many phishing attempts is to gain an employee's login credentials in order to access a company's network, there are industry-standard measures that companies can implement to greatly reduce unauthorized access, even if a phishing attempt is successful. For example, multi-factor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login. This could include entering a code from the user's smartphone, answering a security question, or providing a biometric indicator such as a fingerprint or facial recognition—in addition to entering a username and password. Thus, even if hackers obtain an employee's username and password, access to the

[17] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf (last visited September 20, 2021).
[18] *Id.*

company's system is thwarted because they do not have access to the additional authentication methods.

30. Similarly, companies housing sensitive data must implement adequate "network segmentation," which is the practice of dividing a larger network into several smaller subnetworks that are each isolated from one another to provide enhanced security. For example, hackers that gain access to an unsegmented network (commonly through phishing) can move laterally across the network to access databases containing valuable assets such as sensitive personal information or financial records. Malicious lateral movement can be difficult to detect because it oftentimes appears as normal network traffic. By implementing adequate network segmentation, companies can prevent even those hackers who already gained a foothold in their network from moving across databases to access their most sensitive data.

31. Network segmentation is commonly used in conjunction with the principle of least privilege (POLP), which is a security practice that limits employees' privileges to the minimum necessary to perform the job or task. In an IT environment, adhering to POLP reduces the risk of hackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.[19] In an example given by security software provider Digital Guardian, "an employee whose job is to enter info into a database only needs the ability to add records to that database. If malware infects that employee's computer or if the employee clicks a link in a phishing email, the malicious attack is limited to making database entries. If that employee has root access privileges, however, the infection can spread system-wide."[20] This is why approximately 67% of targeted malware and

[19] https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance (last visited September 20, 2021).
[20] *Id.*

phishing attacks are directed at individual contributors and lower-level management personnel.[21]

32. In addition to addressing "phishing" attempts, the CISA guidance encourages organizations to prevent unauthorized access by:

- Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;
- Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;
- Ensuring devices are properly configured and that security features are enabled;
- Employing best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and
- Disabling operating system network file sharing protocol known as Server Message Block (SMB) which is used by threat actors to travel through a network to spread malware or access sensitive data.[22]

33. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[23]

34. Despite holding the PII of thousands of patients, UC San Diego Health failed to adhere these recommended best practices. It lacked the necessary safeguards to detect and prevent phishing attacks and failed to implement adequate monitoring or control systems to detect the unauthorized infiltration after it occurred. UC San Diego Health, like any healthcare provider its size storing

[21] https://healthitsecurity.com/news/pharmaceutical-companies-most-targeted-industry-by-cybercriminals (last visited September 20, 2020).
[22] CISA Guide at 4.
[23] *Id*. at 5.

valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to thousands of patient files.

35. UC San Diego Health had the knowledge and resources to prevent a breach—and in fact made significant expenditures to promote its growing healthcare practice—but neglected to make corresponding investments in data security to ensure the thousands of sensitive files in its possession were securely stored. UC San Diego Health's implementation of "enhanced" security measures only after the fact is inexcusable given its knowledge that it was a prime target for cyberattacks.

Allegations Relating to Plaintiff Denise Menezes

36. Plaintiff Denise Menezes lives and resides in El Cajon, California and is a patient of Moores Cancer Center where she is being treated for breast cancer.

37. For purposes of receiving medical treatment, Ms. Menezes was required to provide UC San Diego Health with her sensitive personal information, including, among other information, her full name, home address, date of birth, e-mail address, social security number, health insurance ID cards, and driver's licenses.

38. UC San Diego Health also maintained Ms. Menezes' patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, provider names, and medical and clinical treatment information.

39. In September 2021, Ms. Menezes received a notification letter from UC San Diego Health informing her that she was a victim of the Data Breach. The letter stated: "As previously disclosed July 27, 2021, UC San Diego Health recently identified and responded to a security matter involving unauthorized access to some employee email accounts." The letter further stated: "We determined September 1, 2021 that emails or attachments containing some of your personal information were accessed and/or acquired by the unauthorized actor between December 2, 2020 and April 8, 2021, including the following: full name; claims information (date and cost

of health care services and claims identifiers); Medical Record Number and other medical identifiers; treatment information. It does not appear that your personal information was the target of this incident and there is no evidence at this time your personal information was misused."

40. The letter recommended that Ms. Menezes "remain alert to threats of identity theft and fraud . . . by regularly reviewing your financial statements, credit reports, and Explanations of Benefits (EOBs) from your health insurers for any unauthorized activity."

41. UC San Diego Health's letter created more questions than it answered. First, UC San Diego Health misrepresented the fact that it "previously disclosed" the Data Breach, as the vast majority of victims were unaware the Data Breach occurred given that they do not regularly check the UC San Diego Health website and the organization waited months to provide individualized notice. Additionally, UC San Diego Health provided no context for its unsubstantiated statement that it "does not appear that your personal information was the target of this incident" as the objective of almost every data breach is to gain access to an organization's sensitive data so that the data can be misused for financial gain. UC San Diego Health's assertion that "there is no evidence at this time your personal information was misused" was equally dubious as the organization would not receive reports of misuse until it affirmatively notified affected individuals regarding the Data Breach.

42. Furthermore, the letter did not explain the nature of the attack, the identity of the hackers, or the number of individuals affected. UC San Diego Health's decision to withhold these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk. By waiting months to disclose the Data Breach and by downplaying the risk of misuse, UC San Diego Health prevented victims from taking meaningful, proactive, and targeted mitigation measures that could help protect them from harm.

43. As a result of the Data Breach, Ms. Menezes has spent time and effort researching the breach and reviewing her financial and medical account statements for evidence of unauthorized activity, which she will continue to do for years into the future. Ms. Menezes also suffered emotional distress knowing that her highly personal medical and treatment information is now available to criminals to commit blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against her for the rest of her life.

UC San Diego Health Failed to Comply with Federal Law and Regulatory Guidance

44. UC San Diego Health is a healthcare provider covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (*see* 45 C.F.R. § 160.102) and as such 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.

45. These rules establish national standards for the protection of patient information, including PHI, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

46. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[24]

47. HIPAA requires that UC San Diego Health implement appropriate safeguards for this information.[25]

[24] 45 C.F.R. § 164.502.
[25] 45 C.F.R. § 164.530(c)(1).

48. HIPAA requires that UC San Diego Health provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—*i.e*. non-encrypted data.[26]

49. Despite these requirements, UC San Diego Health failed to comply with its duties under HIPAA and its own Notice of Privacy Practices. Indeed, UC San Diego Health failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Adequately protect the PII of its patients and employees;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information 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);

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

f. Implement adequate 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);

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

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary

[26] 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

50. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[27]

51. The FTC's publication *Protecting Personal Information: A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[28] Among other things, the guidelines note that businesses should protect the personal customer information that they collect and store; properly dispose of personal information that is no longer needed; encrypt information stored on their computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[29]

52. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security

[27] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited September 20, 2021).

[28] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited September 20, 2021).

[29] *Id*.

measures.[30] This is consistent with guidance provided by the FBI, HHS, and the principles set forth in the CISA 2020 guidance.

53. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[31]

54. UC San Diego Health was fully aware of its obligation to implement and use reasonable measures to protect the PII of its employees and patients but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. UC San Diego Health's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

The Impact of the Data Breach on Victims

55. The PII exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit medical-related identity theft and fraud, one of the most dangerous and costly forms of identity theft.

56. According to a *Reuters* investigation that included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts, medical data for sale on underground markets "includes names, birth dates, policy numbers, diagnosis codes and billing information" which fraudsters commonly use "to create fake IDs to buy medical equipment or drugs that can be resold, or they

[30] FTC, *Start With Security*, *supra* note 41.

[31] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited September 20, 2021).

combine a patient number with a false provider number and file made-up claims with insurers."[32]

57. According to Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, "Health information is a treasure trove for criminals [because] by compromising it, by stealing it, by having it sold, you have seven to 10 personal identifying characteristics of an individual."[33] For this reason, a patient's full medical records can sell for up to $1,000 on the dark web, while credit card numbers and Social Security numbers may cost $5 or less.[34]

58. As noted by Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies: "The reason for this price discrepancy—like any other good or service—is perceived value. While a credit card number is easily canceled, medical records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information. Once records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient's identity to open credit cards and fraudulent loans."[35]

---

[32] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (last visited September 20, 2021).

[33] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited September 20, 2021).

[34] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited September 20, 2021).

[35] https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited September 20, 2021).

59. Indeed, while federal law generally limits individuals' liability for fraudulent credit card charges to $50, there are no such protections for a stolen medical identity. According to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of $13,500 in out-of-pocket costs to resolve the crime.[36] Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and Medicaid benefits (52%). Only 14% of respondents said that the identity thieves used the information to obtain fraudulent credit accounts, indicating that medical information is a much more profitable market.[37]

60. According to the Ponemon study, "[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate."[38]

61. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with 19% responding that they missed out on employment opportunities as a result.[39]

62. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because HIPAA regulations require the victim to be personally involved in the resolution of the crime.[40] In some cases, victims may not

---

[36] https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 ("Ponemon Study") (last visited September 20, 2021).
[37] *Id*. at 9.
[38] *Id*. at 2.
[39] *Id*. at 14.
[40] *Id*. at 1.

even be able to access medical records using their personal information because they include a false name or data points taken from another person's records. Consequently, only 10% of medical identity theft victims responded that they "achiev[ed] a completely satisfactory conclusion of the incident."[41]

63. Moreover, it can take months or years for victims to even discover they are the victim of medical-related identity theft or fraud given the difficulties associated with accessing medical records and healthcare statements. For example, the FTC notes that victims may only discover their identity has been compromised after they:

- Receive a bill for medical services they did not receive;
- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;
- Find erroneous listings of office visits or treatments on their explanation of benefits (EOB);
- Receive information from their health plan that they have reached their limit on benefits; or
- Be denied insurance because their medical records show a condition they do not have.[42]

64. Perhaps most dangerous, however, is the potential for misdiagnoses or treatment. According to Ann Patterson, a senior vice president of the Medical Identity Fraud Alliance, "About 20 percent of victims have told us that they got the wrong diagnosis or treatment, or that their care was delayed because there was confusion about what was true in their records due to the identity theft." [43] This echoes the Ponemon study, which notes that "many respondents are at risk for

---

[41] *Id.*

[42] https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited September 20, 2021).

[43] https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited September 20, 2021).

further theft or errors in healthcare records that could jeopardize medical treatments and diagnosis."[44]

65. According to a Consumer Reports article entitled *The Rise of Medical Identity Theft*, this outcome "isn't a hypothetical problem" as the "long tail on medical identity theft can create havoc in victims' lives."[45] As one example, a pregnant woman reportedly used a victim's medical identity to pay for maternity care at a nearby hospital. When the infant was born with drugs in her system, the state threatened to take the *victim's* four children away—not realizing her identity had been stolen. The victim ultimately had to submit to a DNA test to remove her name from the infant's birth certificate, but it took years to get her medical records corrected.[46]

66. Other types of medical fraud include "leveraging details specific to a disease or terminal illness, and long-term identity theft."[47] According to Tom Kellermann, "Traditional criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[48] Long-term identity theft occurs when fraudsters combine a victim's data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

67. Given the amount of time hackers had access to UC San Diego Health's systems, many victims of the Data Breach have likely already experienced

---

[44] Ponemon Study at 1.
[45] https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited September 20, 2021).
[46] *Id.*
[47] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited September 20, 2021).
[48] *Id.*

significant harms as the result of the Data Breach, including, but not limited to, medical-related identity theft and fraud. Plaintiff and class members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and healthcare statements, checking credit reports, and spending time and effort searching for unauthorized activity.

68. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft
- 7% reported feeling suicidal.[49]

69. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues)

[49] https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited September 20, 2021).

- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[50]

70. The unauthorized disclosure of the sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm. *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

71. And consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

72. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and class members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their PII;
b. losing the value of the explicit and implicit promises of data security;
c. identity theft and fraud resulting from the theft of their PII;
d. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
e. anxiety, emotional distress, and loss of privacy;

[50] *Id.*

f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their PII being in the possession of one or many unauthorized third parties.

73. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

74. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes. According to the Government Accountability Office, which conducted a study regarding data breaches: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[51]

75. Plaintiff and class members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant,

[51] http://www.gao.gov/new.items/d07737.pdf (last visited September 20, 2021).

approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[52]

76. Because of the value consumers place on data privacy and security, healthcare providers with robust data security practices are viewed more favorably by patients and can command higher prices than those who do not. Consequently, had UC San Diego Health's patients known the truth about its data security practices—that it did not adequately protect and store their PII—they would not have sought medical care from UC San Diego Health or would have paid significantly less. As such, Plaintiff and class members did not receive the benefit of their bargain with UC San Diego Health because they paid for the value of services they did not receive.

77. Plaintiff and class members have a direct interest in UC San Diego Health's promises and duties to protect their PII, *i.e.*, that UC San Diego Health *not increase* their risk of identity theft and fraud. Because UC San Diego Health failed to live up to its promises and duties in this respect, Plaintiff and class members seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by UC San Diego Health's wrongful conduct. Through this remedy, Plaintiff and class members seek to restore themselves and class members as close to the same position as they would have occupied but for UC San Diego Health's wrongful conduct, namely its failure to adequately protect Plaintiff's and class members' PII.

78. Plaintiff and class members further seek to recover the value of the unauthorized access to their PII permitted through UC San Diego Health's wrongful

[52] https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited September 20, 2021).

conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a nonpracticing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and class members have a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

79. Because UC San Diego Health continues to hold the PII of its patients, Plaintiff and class members have an interest in ensuring that their PII is secured and not subject to further theft.

CLASS ACTION ALLEGATIONS

80. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Federal Rule of Civil Procedure 23 and as a representative of the Classes defined as follows:

(a) **The Nationwide Class:** All U.S. residents whose personal information was compromised in the Data Breach.

(b) **The California Class:** All California citizens whose personal information was compromised in the Data Breach.

81. Specifically excluded from the Classes are Defendant; its officers, directors, or employees; any entity in which Defendant has a controlling interest;

and any affiliate, legal representative, heir, or assign of Defendant. Also excluded from the Classes are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

82. Class Identity: The members of the Classes are readily identifiable and ascertainable. Defendant and/or its affiliates, among others, possess the information to identify and contact class members.

83. Numerosity: The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of class members is unknown to Plaintiff at this time, the Classes contain thousands of individuals whose data was compromised in the Data Breach.

84. Typicality: Plaintiff's claims are typical of the claims of the members of the classes because all class members had their PII compromised in the Data Breach and were harmed as a result.

85. Adequacy: Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has no interest antagonistic to those of the classes and are aligned with Class members' interests because Plaintiff was subject to the same Data Breach as class members and faces similar threats due to the Data Breach as class members. Plaintiff has also retained competent counsel with significant experience litigating complex class actions, including Data Breach cases involving multiple classes and data breach claims.

86. Commonality and Predominance: There are questions of law and fact common to the classes. These common questions predominate over any questions affecting only individual class members. The common questions of law and fact include, without limitation:

a. Whether Defendant violated § 1798.150 of the CCPA;

b. Whether Defendant owed Plaintiff and class members a duty to implement and maintain reasonable security procedures and practices to protect their PII;

c. Whether Defendant breached an express or implied contract with Plaintiff and class members, including whether Defendant breached an agreement with Plaintiff and class members to keep their PII confidential;

d. Whether Defendant received a benefit without proper restitution making it unjust for Defendant to retain the benefit without commensurate compensation;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiff's and class members' PII;

f. Whether Defendant Plaintiff's its duty to implement reasonable security systems to protect Plaintiff's and class members' PII;

g. Whether Defendant's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and class members;

h. Whether Defendant adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

i. Whether Plaintiff and class members are entitled to credit monitoring and other injunctive relief;

j. Whether Defendant provided timely notice of the Data Breach to Plaintiff and class members; and,

k. Whether class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

87. Defendant has engaged in a common course of conduct and class members have been similarly impacted by Defendant's failure to maintain reasonable security procedures and practices to protect customers' PII, as well as Defendant's failure to timely alert affected customers to the Data Breach.

88. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under Federal Rule of Civil Procedure 23.

CLAIMS FOR RELIEF

COUNT I

Violation of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code § 1798.150
(On Behalf of the California Class)

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

90. Although the University of California, San Diego, is a 501(c)(3) organization that is exempt from federal income tax, UC San Diego Health qualifies as a "business" as defined in § 1798.140(c)(1) of the CCPA because it is an association or other legal entity consisting of a health care system that is operated for the profit or financial benefit of its owners, the Regents of the University of California, generating annual gross revenues exceeding $25 million. Defendant collects consumers' PII as defined under the CCPA.

91. Defendant 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 Defendant's violations of its duty to

implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

92. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and class members' PII. As detailed herein, Defendant failed to do so. As a direct and proximate result of Defendant's acts, Plaintiff's and class members' PII, including full names in conjunction with medical information, was subjected to unauthorized access and exfiltration, theft, or disclosure.

93. Plaintiff and class members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Plaintiff's and class members' PII. Plaintiff and class members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

94. Pursuant to Cal. Civ. Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendant's registered service agent, detailing the specific provisions of the CCPA that Defendant has and continues to violate. If Defendant cannot cure within 30 days, which Plaintiff believes is not possible under these facts and circumstances, then Plaintiff intends to amend the Complaint to seek statutory damages as permitted by the CCPA.

95. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the personal information under the CCPA.

96. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

COUNT II

Violation of California's Confidentiality of Medical Information Act ("CMIA")
Cal. Civ. Code § 56, *et seq*.
(On Behalf of the California Class)

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

98. Defendant is a "provider of healthcare" pursuant to Cal. Civ. Code § 56.06, and is subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a) and (e), 56.36, 56.101.

99. Plaintiff and class members are "patients" as defined in the CMIA, Cal. Civ. Code § 56.05(k).

100. 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 Data Breach occurred when an employee or employees of Defendant affirmatively granted access to confidential emails, attachments, and the PII contained therein, to unauthorized individuals by responding to their phishing attempts. This disclosure was exacerbated by Defendant's previous failure to implement reasonable and adequate data security measures and protocols to protect Plaintiff's and class members' PII.

101. 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 violated the CMIA, Cal. Civ. Code §§ 56.06 and 56.101(a). By Defendant's own admission, confidential medical information contained in unencrypted emails and attachments has been accessed and viewed by an unauthorized third party or parties. Accordingly, Defendant's systems and protocols did not protect and preserve the

integrity of electronic medical information in violation of the CMIA, Cal. Civ. Code § 56.101.

102. Plaintiff and class members 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 Cal. Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses and costs.

COUNT III

Violation of California's Unfair Competition Law ("UCL") Cal. Bus. Prof. Code § 17200, *et seq*. *(On Behalf of the California Class)*

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

104. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

105. Defendant violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

106. Defendant's "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff and class members' PII from unauthorized disclosure, release, breaches, and theft, which was a direct and proximate cause of the Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. For example, Defendant failed to implement sufficient training and security protocols to detect and prevent "phishing" attacks, failed to mandate strong passwords and use of two-factor authentication, and failed to adequately monitor its network activity. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and class members, whose PII has been compromised.

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in state and federal laws including the FTC Act, 15 U.S.C. § 45; HIPAA, 42 U.S.C. § 1302d, *et seq.*; the CCPA, Cal. Civ. Code § 1798.150; the CMIA, Cal. Civ. Code § 56, *et seq.*; and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

c. Defendant's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's grossly inadequate security, consumers could not have reasonably avoided the harms that Defendant caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

107. Defendant has engaged in "unlawful" business practices by violating multiple state and federal laws, including the FTC Act, 15 U.S.C. § 45; HIPAA, 42 U.S.C. § 1302d, *et seq.*; the CCPA, Cal. Civ. Code § 1798.150; the CMIA, Cal. Civ. Code § 56, *et seq.*; California's Consumer Records Act, Cal. Civ. Code § 1798.81.5; and California common law.

108. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' PII;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and class members' PII.

109. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of patients' PII.

110. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and class members were injured and lost money or property, the premiums and/or price received by Defendant for its goods and services, the loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

111. Defendant acted intentionally, knowingly, and maliciously to violate the UCL, and recklessly disregarded Plaintiff and class members' rights. Defendant's past data breaches and other breaches within the industry put it on notice that its security and privacy protections were inadequate.

112. Plaintiff and class members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's

unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT IV

Negligence

(On Behalf of the Nationwide Class or Alternatively the California Class)

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

114. Defendant required Plaintiff and class members to provide their PII as a condition of receiving healthcare and medical services. Defendant collected and stored the data for purposes of providing medical treatment as well as for commercial gain.

115. Defendant owed Plaintiff and class members a duty to exercise reasonable care in protecting their PII from unauthorized disclosure or access. Defendant acknowledged this duty in its Notice of Privacy Policy, where it promised not to disclose Plaintiff's and class members' PII.

116. Defendant owed a duty of care to Plaintiff and class members to provide security, consistent with industry standards, to ensure that Defendant's systems and networks adequately protected the PII.

117. As a healthcare provider, Defendant had a special relationship with Plaintiff and class members who entrusted Defendant to adequately their confidential personal, financial, and medical information.

118. Defendant's duty to use reasonable care in protecting PII arose as a result of the parties' relationship, as well as common law and federal law, including the HIPAA regulations described above and Defendant's own policies and promises regarding privacy and data security.

119. Defendant knew, or should have known, of the risks inherent in collecting and storing PII in a centralized location, Defendant's vulnerability to phishing attacks, and the importance of adequate security.

120. Defendant breached its duty to Plaintiff and class members in numerous ways, as described herein, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiff and class members;

b. Failing to comply with industry standard data security measures for the healthcare industry leading up to the Data Breach;

c. Failing to comply with its own privacy policies;

d. Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;

e. Failing to adequately monitor, evaluate, and ensure the security of Defendant's network and systems;

f. Failing to recognize in a timely manner that PII had been compromised; and

g. Failing to timely and adequately disclose the Data Breach.

121. Plaintiff and class members' PII would not have been compromised but for Defendant's wrongful and negligent breach of their duties.

122. Defendant's failure to take proper security measures to protect the sensitive PII of Plaintiff and class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of PII by unauthorized third parties. Given that healthcare providers are prime targets for hackers, Plaintiff and class members are part of a foreseeable, discernible group that was at high risk of having their PII misused or disclosed if not adequately protected by Defendant.

123. It was also foreseeable that Defendant's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiff and class members.

124. As a direct and proximate result of Defendant's conduct, Plaintiff and class members have and will suffer damages including: (i) the loss of rental or use value of their PII; (ii) the unconsented publication of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; and (ix) any nominal damages that may be awarded.

COUNT V

Negligence *Per Se*

(On Behalf of the Nationwide Class or Alternatively the California Class)

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

126. As a healthcare provider, Defendant is covered by HIPAA, 45 C.F.R. § 160.102, and is therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

127. 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information," and Subpart E governing "Privacy of Individually Identifiable Health Information."

128. 45 C.F.R. § 164.104 states that the "standards, requirements, and implementation specifications adopted under this part" apply to covered entities and their business associates, such as Defendant.

129. Defendant is obligated under HIPAA to, among other things, "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information." 45 C.F.R. § 164.306.

130. 45 C.F.R. Sections 164.308 (Administrative safeguards), 164.310 (Physical safeguards), 164.312 (Technical safeguards), 164.314 (Organizational requirements), and 164.316 (Policies and procedures and documentation requirements) provide mandatory standards that all covered entities must adhere to.

131. Defendant violated HIPAA by failing to adhere to and meet the required standards as set forth in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

132. Likewise, HIPAA regulations require covered entities "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach" to "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of" a data breach. 45 C.F.R. § 164.404. The notice must also contain a minimum amount of information regarding the breach (including the dates of the breach and its discovery), the types of protected health

information that were involved, steps individuals should take to protect themselves from harm resulting from the breach, a description of what the entity is doing to investigate the breach and mitigate harm, and contact information to obtain further information. *Id*.

133. Defendant breached its notification obligations under HIPAA by failing to give timely and complete notice of the breach to Plaintiff and class members.

134. HIPAA requires 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). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

135. HIPAA further requires Defendant to disclose the unauthorized access and theft of the PII to Plaintiff and class members "without unreasonable delay" so that Plaintiff and class members can take appropriate measures to mitigate damages, protect against adverse consequences, and detect misuse of their PII. See 45 C.F.R. § 164.404.

136. Defendant violated HIPAA by failing to reasonably protect Plaintiff's and class members' PII and by failing to give complete and forthright notice, as described herein.

137. Defendant's violations of HIPAA constitute negligence *per se*.

138. Plaintiff and class members are within the class of persons that HIPAA and its implementing regulations were intended to protect.

139. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

140. Additionally, Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such

as Defendant, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1).

141. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

142. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with applicable industry standards. Defendant's conduct was unreasonable given the nature and amount of PII they obtained, stored, and disseminated in the regular course of their business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiff and class members.

143. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

144. Plaintiff and class members are within the class of persons that the FTC Act was intended to protect.

145. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and class members.

146. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and class members have suffered, continue to suffer, and will suffer, injuries, damages, and harm as alleged herein.

COUNT VI

Breach of Contract

(On Behalf of the Nationwide Class or Alternatively the California Class)

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

148. Defendant disseminated a "Notice of Privacy Practices" ("Privacy Notice") and "Patient Rights and Responsibilities" ("Patient Rights Notice") to its patients, which each constitute an agreement between Defendant and persons who provided their PII to Defendant, including Plaintiff and class members.

149. Plaintiff and class members formed a contract with Defendant and complied with all obligations under such contract when they provided PII to Defendant subject to the Privacy Notice and/or Patient Rights Notice.

150. Defendant promised in the Privacy Notice that it would "follow the legal duties and privacy practices described in this notice" which included a promise not to disclose information unless as authorized. Defendant promised in the Patient Rights Notice that its patients have a right to "[c]onfidential treatment of all communications and records pertaining to your care and stay in the hospital."

151. Defendant breached its agreements with Plaintiff and class members when Defendant allowed for the disclose of Plaintiff's and class members' PII without their authorization and in a manner that was inconsistent with the permissible authorizations set forth in the Privacy Notice, as well as when it failed to maintain the confidentiality of Plaintiff's and class members' medical and treatment information.

152. As a direct and proximate result of these breaches, Plaintiff and class members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiff and class members alternatively seek an award of nominal damages.

COUNT VII

Breach of Implied Contract

(On Behalf of the Nationwide Class or Alternatively the California Class)

153. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs and asserts this claim in the alternative to Plaintiff's breach of express contract claim to the extent necessary.

154. Plaintiff and class members were required to provide their PII to Defendant in order to receive healthcare services and treatment.

155. As part of these transactions, Defendant agreed to safeguard and protect the PII of Plaintiff and class members. Implicit in these transactions between Defendant and class members was the obligation that Defendant would use the PII for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

156. Additionally, Defendant implicitly promised to retain this PII only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the PII of Plaintiff and class members from unauthorized disclosure or access.

157. Plaintiff and class members entered into implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and class members believed that Defendant would use part of the monies paid to Defendant under the implied contracts to fund adequate and reasonable data security practices to protect their PII.

158. Plaintiff and class members would not have provided and entrusted their PII to Defendant or would have paid less for Defendant's services in the absence of the implied contract between them and Defendant. The safeguarding of Plaintiff's and class members' PII was critical to realizing the intent of the parties.

159. The nature of Defendant's implied promise itself—the subject matter of the contractual provision at issue—was to protect Plaintiff's and class members' PII in order to prevent harm and prevent present and continuing increased risk.

160. Defendant breached their implied contract with Plaintiff and class members by failing to reasonably safeguard and protect Plaintiff's and class members' PII, which was compromised as a result of the Data Breach.

161. As a direct and proximate result of Defendant's breaches, Plaintiff and class members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiff and class members alternatively seek an award of nominal damages.

COUNT VIII

Unjust Enrichment/Quasi-Contract

(On Behalf of the Nationwide Class or Alternatively the California Class)

162. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs and asserts this claim in the alternative to Plaintiff's breach of contract claims to the extent necessary.

163. Plaintiff and class members have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by the Defendant and which was stolen in the Data Breach. This information has independent value.

164. Plaintiff and class members conferred a monetary benefit on Defendant in the form of payments for medical and healthcare services, including those paid indirectly by Plaintiff and class members to Defendant.

165. Defendant appreciated and had knowledge of the benefits conferred upon it by Plaintiff and class members.

166. The price for medical and healthcare services that Plaintiff and class members paid (directly or indirectly) to Defendant should have been used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

167. Likewise, in exchange for receiving Plaintiff's and class members' valuable PII, which Defendant was able to use for their own business purposes and which provided actual value to Defendant, Defendant was obligated to devote sufficient resources to reasonable data privacy and security practices and procedures.

168. As a result of Defendant's conduct, Plaintiff and class members suffered actual damages as described herein. Under principals of equity and good conscience, Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and class members all unlawful or inequitable proceeds they received from Plaintiff and class members, including damages equaling the difference in value between medical and healthcare services that included implementation of reasonable data privacy and security practices that Plaintiff and class members paid for and the services without reasonable data privacy and security practices that they actually received.

COUNT IX

Breach of Confidence

(On Behalf of the Nationwide Class or Alternatively the California Class)

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

170. Defendant required Plaintiff and class members to provide their PII as a condition of receiving healthcare and medical treatment. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

171. Defendant knew Plaintiff's and class members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreed to protect the confidentiality and security of the PII it collected, stored, and maintained.

172. There was disclosure of Plaintiff's and class members' PII as a result of the Data Breach in violation of this understanding. The disclosure occurred because Defendant failed to implement and maintain reasonable safeguards to protect its patients' PII and failed to comply with industry-standard data security practices.

173. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and class members suffered injury and sustained actual losses and damages

as alleged herein. Plaintiff and class members alternatively seek an award of nominal damages.

COUNT X

Declaratory Judgment
(On Behalf of the Nationwide Class)

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

175. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

176. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and class members from further cyberattacks and data breaches that could compromise their PII.

177. Defendant still possesses PII pertaining to Plaintiff and class members, which means their PII remains at risk of further breaches because Defendant's data security measures remain inadequate. Plaintiff and class members continue to suffer injuries as a result of the compromise of their PII and remain at an imminent risk that additional compromises of their PII will occur in the future.

178. Pursuant to the Declaratory Judgment Act, Plaintiff seeks a declaration that: (a) Defendant's existing data security measures do not comply with its obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) Defendant must have policies and procedures in place to ensure the parties with whom it shares sensitive personal information maintain reasonable, industry-standard security measures, including, but not limited to, those listed at (ii),

(a)-(i), *infra*, and must comply with those policies and procedures; (2) Defendant must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiff's and class members' PII if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

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

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Encrypting PII and segmenting PII by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of its systems;

e. Purging, deleting, and destroying in a reasonable and secure manner PII not necessary to perform essential business functions;

f. Conducting regular database scanning and security checks;

g. Conducting regular employee education regarding best security practices;

h. Implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and

i. Routinely and continually conducting 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.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the classes set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representatives and Plaintiff's counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of their unlawful acts, omissions, and practices;

F. That Plaintiff be granted the declaratory and injunctive relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial in the instant action.

Dated: September 20, 2021

/s/ *Jason S. Hartley*
Jason S. Hartley (SBN 192514)
HARTLEY LLP
101 West Broadway, Suite 820
San Diego, California 92101
Tel: 619-400-5822
hartley@hartleyllp.com

Norman E. Siegel*
J. Austin Moore*
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel: 816-714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
**Pro Hac Vice Forthcoming*

Counsel for Plaintiff and the Class

ClassAction.org
