Gayle M. Blatt, SBN 122048
gmb@cglaw.com
Jeremy Robinson, SBN 188325
jrobinson@cglaw.com
P. Camille Guerra, SBN 326546
camille@cglaw.com
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232

Counsel for Plaintiff
Richard Hartley

[Additional Counsel Listed on Signature Page]

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

RICHARD HARTLEY, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA d/b/a UC SAN DIEGO HEALTH, a public entity, and DOES 1 through 50,

Defendants.

Case No.: '21CV1668 H KSC

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Richard Hartley ("Plaintiff" or "Hartley") brings this Class Action Complaint against The Regents of The University of California d/b/a UC San Diego Health ("UC San Diego Health") and Does 1 through 50 (collectively "Defendants") in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

Introduction

1. UC San Diego Health is the academic health system of the University of California, San Diego. It is the only academic health system serving San Diego and has one of only two adult Level I trauma centers in the region. UC San Diego Health offers inpatient and specialty care in La Jolla and Hillcrest, as well as primary, urgent and express care at clinics located throughout the region. UC San Diego Health is a referral center for complex, specialty care that is beyond the breadth and scope of most community hospitals. UC San Diego Health's community members include patients, employees, and students.

2. UC San Diego Health is owned, operated, managed, and controlled by Defendants Regents of the University of California.

3. Defendants Does 1 through 50 are employees or agents, either actual or ostensible, of Regents of the University of California. At all times herein alleged, Does 1 through 50 were acting in the course and scope of their employment or agency with the Regents. Defendants Does 1 through 50 are liable herein under Government Code § 820 as well as under other applicable statues. Defendants UC San Diego Health is liable herein for the acts and omissions of Does 1 through 50 under Government Code § 815.2 as well as other applicable statutes.

4. On July 27, 2021, Defendants announced a security incident involving the theft of sensitive personally identifiable information ("PII") and protected health information ("PHI") of their patients, employees, and students (collectively, "Sensitive Information").[1] The stolen Sensitive Information included full name, address, date of birth, email, fax number, claims information (date and cost of health care services and claims identifiers), laboratory results, medical diagnosis and conditions, Medical Record Number and other medical identifiers, prescription information, treatment information, medical information, Social Security number, government identification number, payment card number or financial account number and security code, student ID number, and username and password. (the "Data Breach").

5. Although the Data Breach began on December 2, 2020, and Defendants discovered it on March 12, 2021, the unauthorized access was not terminated until April 8, 2021. Defendants then waited several months before beginning to notify patients and employees.

---

[1] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.* ("HIPAA"), protected health information ("PHI") is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, available at: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Sept. 21, 2021).

6. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Sensitive Information.

7. Defendants disregarded the rights of Plaintiff and Class Members (defined below) by, among other things, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have reasonable or adequately robust computer systems and security practices to safeguard patients' Sensitive Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

8. As a result of Defendants' failure to implement and follow reasonable security procedures, the Sensitive Information of Plaintiff and the Class is now in the hands of thieves. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach and will forever be at a present and continuing risk of identity theft and fraud.

9. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence; invasion of privacy; breach of implied contract; unjust enrichment; breach of fiduciary duty; breach of confidence; violation of the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq*. (§ 1798.150(a))); and violation of the Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq*.). Plaintiff and the Class Members seek to compel Defendants to adopt reasonably sufficient security practices to safeguard patients' Sensitive Information that remains

in Defendants' custody to prevent incidents like the Data Breach from reoccurring in the future.

Parties

10. Plaintiff Richard Hartley is a resident of the state of California and a former UC San Diego Health patient. On or about September 9, 2021, Plaintiff Hartley received notice from UC San Diego Health that his Sensitive Information had been improperly exposed to unauthorized third parties.

11. The University of California is a "public trust ... with full powers of organization and government." Cal. Const., art. IX, § 9, subd. (a). It is administered by the corporation known as "The Regents of the University of California." UC San Diego Health is the health system of the University of California, San Diego, and a medical provider throughout San Diego.

12. The true names and capacities, whether individual or otherwise, of defendants Does 1 to 50 are unknown to Plaintiff who, therefore, sues them by such fictitious names under Code of Civil Procedure § 474. Plaintiff is informed and believes that each of the defendants is responsible in some manner for the acts or omissions alleged in this complaint or caused him damages.

13. At all times herein mentioned, each defendant was acting in the course and scope of his or her employment with the other defendants. Defendants are therefore vicariously liable for the acts of each of the remaining defendants herein.

14. In addition, each defendant was at all times acting as the ostensible agent of the remaining defendants and was doing so at the behest of and with the approval of those defendants. At all times herein relevant, Plaintiff reasonably and without negligence relied on the

representations made by the defendants about the agency and employment of each of the remaining defendants.

Jurisdiction and Venue

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

16. Plaintiff Hartley's Sensitive Information was maintained in this District and this District is where the Data Breach happened, which led him to sustain damage. Through its business operations in this District, UC San Diego Health intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District. Defendants are based in this District, they maintain Sensitive Information in this District, and they have caused harm to Plaintiff and Class Members in this District.

Statement of Facts

A. Background.

18. UC San Diego Health has been in operation since 1966, it comprises the UC San Diego Medical Center in Hillcrest as well as the; Jacobs Medical Center; Moores Cancer Center; Shiley Eye Institute; Sulpizio Cardiovascular Center, and Koman Family Outpatient Pavilion, all in La Jolla. It also includes several outpatient sites located throughout San Diego County. The health system works closely with the university's School of Medicine and Skaggs School of Pharmacy to provide training to medical and pharmacy students and advanced clinical care to patients.

UC San Diego Health is repeatedly ranked the No. 1 health care system in San Diego.

19. As a part of providing health services, employment, or student services, Defendants UC San Diego Health and Does 1 through 50 require patients and other persons to provide a significant amount of PII. In addition, Defendants both collect and generate PHI.

20. Patients and healthcare professionals can request and receive medical records online through MyUCSDChart though UC San Diego Health's online portal and have the results sent to the doctor or directly to the patient. Patients are billed through their healthcare insurance or personally. Due to the nature of these services, Defendants must keep patients' Sensitive Information in its system. Defendants accomplish this by keeping the Sensitive Information electronically—even in their email systems, as evidenced by this Data Breach.

21. Plaintiff and Class Members rightfully demand security to safeguard their Sensitive Information. As a healthcare provider, employer, and educational institution, UC San Diego Health is required to ensure that such sensitive, personal information is not disclosed or disseminated to unauthorized third parties without the parties' express, written consent, as further detailed below.

B. The Data Breach.

22. On or about December 2, 2020, unauthorized malicious actors gained access to certain of Defendants' systems using a phishing attack. Once that access was obtained, those malicious actors had easy access to the Sensitive Information stored by Defendants.

23. For approximately the next four months, until April 8, 2021, these malicious actors viewed and exfiltrated Plaintiff's and the Class's Sensitive Information. Although Defendants discovered suspicious

activity on their systems on March 12, 2021, it took until April for them to identify it as a "security matter." Finally, on April 8, 2021, Defendants expelled the intruders from their systems.

24. On or around July 27, 2021, Defendants posted a notice of the Data Breach on their website. Beginning on or about September 9, 2021, Defendants sent an undisclosed number of patients, employees, and students a Notice of Data Breach. UC San Diego Health website also issued a Substitute Notice of Data Breach on that same date.

25. UC San Diego Health's patients' Sensitive Information is likely for sale on the dark web and, on information and belief, is still for sale to criminals. This means that the Data Breach was successful; unauthorized individuals accessed UC San Diego Health's patients' and employees' unencrypted, unredacted information, including name, date of birth, billing and insurance information, patient referral information, relevant medical records, and more, including Social Security Numbers.

C. Mr. Hartley's Efforts to Secure His Sensitive Information

26. Upon receiving Notice from UC San Diego Health on or about September 9, 2021, Plaintiff Hartley checked his credit reports as well as his banking statements and credit card statements. Plaintiff Hartley will continue to monitor his financial accounts as well as his healthcare information. This is time Plaintiff Hartley otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

27. Knowing that thieves stole his Sensitive Information and knowing that his Sensitive Information may be available for sale on the dark web, has caused Plaintiff Hartley great anxiety. He is now very concerned about his healthcare coverage and identity theft in general. This Data Breach has given Plaintiff Hartley hesitation about using electronic

services, and reservations about conducting other online activities requiring his personal information.

28. Plaintiff Hartley suffered actual injury from having his Sensitive Information exposed as a result of the Data Breach including, but not limited to: (a) paying monies to Defendants for their goods and services which he would not have had Defendants disclosed that they lacked data security practices adequate to safeguard consumers' Sensitive Information from theft; (b) damages to and diminution in the value of his Sensitive Information—a form of intangible property that the Plaintiff Hartley entrusted to Defendants as a condition for healthcare services; (c) loss of his privacy; and (d) imminent and impending injury arising from the present and continuing risk of fraud and identity theft; (e) the time and expense of mitigation efforts as a result of the Data Breach.

29. As a result of the Data Breach, Plaintiff Hartley will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

D. UC San Diego Health's Information Security Statement and Privacy Policies.

30. UC San Diego Health maintains policies that detail their promises and legal obligations to maintain and protect patients' Sensitive Information.

University of California San Diego Health System[2] provides, in part:

UC San Diego Health

---

[2] *UC San Diego Notice of Privacy Practices, available at*: https://health.ucsd.edu/hipaa/Pages/hipaa.aspx (last accessed September 21, 2021).

> UC San Diego Health is one of the health care components of the University of California. The University of California health care components consist of the UC medical centers, the UC medical groups, clinics and physician offices, the UC schools of medicine and other UC health professional schools. The administrative and operational units supporting the provision of care at all locations listed are also health care components of the University of California.
>
> Our Pledge Regarding Your Health information
>
> 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.

31. Health Information Exchange (HIE) at UC San Diego Health information provides, in part[3]:

> If you are a patient at UC San Diego Health, your electronic health information is automatically enrolled in a health information exchange so that your vital health data can be securely made available to doctors – no matter where you receive care.
>
> By participating in a health information exchange, doctors and other health care personnel are permitted to use and share your health information through a health exchange network for HIPAA-permitted purposes only.

[3] https://health.ucsd.edu/patients/san-diego-beacon/Pages/frequently-asked-questions.aspx

> Your electronic health information is made accessible only to doctors and health care personnel providing you with medical care. Your electronic health information is stored only within each treating provider's secure electronic medical record system.
>
> The two health information exchanges that UC San Diego Health participates in only store your identifying information and some markers about where you have received care. The health information exchanges do not store any clinical information about you. They are only a means of exchanging information.
>
> How does UC San Diego Health ensure the privacy and security of my health information, especially when it is being transferred or exchanged?
>
> Your health information is protected by advanced systems that use many security measures. All systems must comply with the privacy and security provisions of HIPAA and similar state laws that may apply.

32. UC San Diego Health also describes how it may use and disclose medical information for each category of uses or disclosures, none of which provide it a right to expose patients' Sensitive Information in the manner it was exposed to unauthorized third parties in the Data Breach.

E. The Healthcare Sector is Particularly Susceptible to Cyber Attacks.

33. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches

from the previous year.[4] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase.[5] That trend continues.

34. Defendants had knowledge and understood that unprotected or exposed Sensitive Information in the care of healthcare companies, such as UC San Diego Health, is valuable and highly sought after by nefarious third parties seeking to illegally monetize it by unauthorized accessing of it. In fact, the healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[6] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on health-care breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[7] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event.

---

[4] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), (last accessed Sept. 21, 2021).

[5] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/2017-data-breaches/ (last accessed Sept. 21, 2021).

[6] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last accessed Sept. 21, 2021).

[7] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed Sept. 21, 2021).

Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[8]

35. Healthcare related data breaches have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[9] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[10]

36. As healthcare providers, Defendants knew, or should have known, the importance of safeguarding the patients' Sensitive Information entrusted to them and of the foreseeable consequences if their data security systems were breached. This includes the significant costs that would be imposed on Defendants' patients, employees, and students as a

---

[8] *Id.*

[9] *2019 HIMSS Cybersecurity Survey, available at*: https://www.himss.org/2019-himss-cybersecurity-survey (last accessed Sept. 21, 2021).

[10] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed Sept. 21, 2021).

result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

F. Defendants Acquire, Collect, and Store Plaintiff's and Class Members' PII/PHI.

37. Defendants acquire, collect, and store a massive amount of its patients', employees', and students' protected health-related information and other personally identifiable data.

38. As a condition of engaging in health services, employment, or student services, Defendants requires that these persons entrust them with highly confidential Sensitive Information.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Sensitive Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Sensitive Information from disclosure.

40. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Sensitive Information. Plaintiff and the Class Members, as current and former patients, relied on Defendants to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

G. The Value of PII and the Effects of Unauthorized Disclosure.

41. Defendants were well aware that the Sensitive Information they collect is highly sensitive and of significant value to those who would use it for wrongful purposes.

42. Sensitive Information is a valuable commodity to identity thieves. As the FTC recognizes, PII and PHI identity thieves can commit

an array of crimes including identify theft, medical and financial fraud.[11] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

43. While credit card information and associated PII and PHI can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute. This is because one's personal health history (e.g., ailments, diagnosis, surgeries, etc.) cannot be changed.[12] PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

44. The ramifications of Defendants' failure to keep its patients', employees', and students' Sensitive Information secure are long lasting and severe. Once Sensitive Information is stolen, fraudulent use of that information and damage to victims may continue for years.

45. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Sensitive Information and of the foreseeable consequences if their data security systems were breached, including the significant costs that would be imposed on Plaintiff and the Class as a result of a breach.

---

[11] Federal Trade Commission, *What To Know About Identity Theft, available at:* https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Sept. 21, 2021).

[12] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at:* https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last accessed Sept. 21, 2021).

H. Defendants' Conduct Violates HIPAA.

46. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[13]

47. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII and PHI like the data Defendants left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

48. Defendants' Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations. Defendants' security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendants creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those

---

[13] HIPAA Journal, *What is Considered Protected Health Information Under HIPAA?*, *available at:* https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/ (last accessed Sept. 21, 2021).

persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

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

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

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronically 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);

g. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

h. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

i. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of

protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

I. Defendants Failed to Comply with FTC Guidelines.

49. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

50. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[15] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

51. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit

---

[14] Federal Trade Commission, *Start With Security*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Sept. 21, 2021).

[15] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Sept. 21, 2021).

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 measures.[16]

52. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, 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 ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

53. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients', employees', and students' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

54. Defendants were at all times fully aware of their obligation to protect the Sensitive Information of patients, employees, and students because of their position as a healthcare provider, employer, and teaching facility. Defendants were also aware of the significant repercussions that would result from their failure to do so.

J. Defendants Failed to Comply with Healthcare Industry Standards.

55. HHS's Office for Civil Rights ("DHHS") notes:

---

[16] FTC, *Start With Security*, *supra* note 16.

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly sensitive and valuable data.[17]

56. DHHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of PII and PHI; (b) educating and training healthcare employees on how to protect PII and PHI; and (c) correcting the configuration of software and network devices.

57. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because of the value of the PII and PHI which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[18] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of PII and PHI.

58. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry,

---

[17] HIPAA Journal, Cybersecurity Best Practices for Healthcare Organizations, https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last accessed Sept. 21, 2021).

[18] *See e.g.*, INFOSEC, *10 Best Practices For Healthcare Security, available at:* https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref (last accessed Sept. 21, 2021).

Defendants chose to ignore them. These best practices were known, or should have been known by Defendants, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Sensitive Information.

K. Plaintiff and Class Members Suffered Damages.

59. The ramifications of Defendants' failure to keep Plaintiff's and the Class's Sensitive Information secure are long lasting and severe. Once PII and PHI is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[19]

60. The Sensitive Information belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendants who did not obtain Plaintiff's or Class Members' consent to disclose such Sensitive Information to any other person as required by applicable law and industry standards.

61. The Data Breach was a direct and proximate result of Defendants' failure to: (a) properly safeguard and protect Plaintiff's and Class Members' Sensitive Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Sensitive Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

---

[19] , *available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Sept. 21, 2021).

62. Defendants had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite their obligation to protect patient data.

63. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Sensitive Information.

64. As a direct and proximate result of Defendants' wrongful actions and inactions, Plaintiff's and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

65. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[20]

66. In the breach notification letter, Defendants made an ambiguous and vague offer of identity monitoring services to patients without providing information as to the terms of service, benefits offered, or length of service. This is wholly inadequate to compensate Plaintiff and

---

[20] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed Sept. 21, 2021).

Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff' and Class Members' Sensitive Information.

67. As a result of the Defendants' failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at a present and continuing risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Sensitive Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from 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 identity theft and fraud;

d. The continued risk to their Sensitive Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fails to undertake appropriate measures to protect the Sensitive Information in their possession; and

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

68. In addition to a remedy for the economic harm, Plaintiff and the Class Members maintain an undeniable interest in ensuring that their Sensitive Information is secure, remains secure, and is not subject to further misappropriation and theft.

L. Defendants' Delay in Identifying & Reporting the Breach Caused Additional Harm.

69. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[21]

70. Indeed, once a data breach has occurred:

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills, insurance invoices, and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves (internal citations omitted).[22]

---

[21] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire¸ *available at:* https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last accessed Sept. 21, 2021).

[22] Consumer Reports, *The Data Breach Next Door Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too*, January 31, 2019, *available at:*

71. Although their Sensitive Information was improperly exposed, viewed, and eventually stolen beginning on or about December 2, 2020, affected persons were not notified of the Data Breach until, at the earliest, late July, 2021 and often not until September, 2021, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

72. As a result of Defendants' delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher.

Class Allegations

73. Plaintiff brings this class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

74. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All individuals whose Sensitive Information was compromised in the data breach first announced by UC San Diego Health on or about July 27, 2021 (the "Nationwide Class").**

75. The California Subclass that Plaintiff seeks to represent is defined as follows:

> **All individuals in the State of California whose Sensitive Information was compromised in the data breach first announced by UC San Diego Health on or about July 27, 2021 (the "California Subclass").**

---

https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed Sept. 21, 2021).

76. Both the Nationwide Class and California Subclass will be referred to as "the Class" except where necessary to distinguish them.

77. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

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

79. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class and California Subclass are so numerous that joinder of all members is impracticable. Defendants have identified thousands of patients, employees, and students whose Sensitive Information may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendants' records.

80. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and when Defendants actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or

obtaining their Sensitive Information;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Members' Sensitive Information;

e. Whether Defendants acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' Sensitive Information;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class Members' Sensitive Information secure and prevent loss or misuse of that Sensitive Information;

g. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendants caused Plaintiff and Class Members damages;

i. Whether Defendants violated the law by failing to promptly notify Class Members that their Sensitive Information had been compromised;

j. Whether Plaintiff and the other Class Members are entitled to actual damages, credit monitoring, and other monetary relief;

k. Whether Defendants violated the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq*. (§ 1798.150(a));

l. Whether Defendants violated the Confidentiality of Medical Information Act (Cal. Civ. Code § 56, *et seq*.); and

81. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

82. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

83. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

84. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and

without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large entities like Defendants. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

85. The nature of this action and the nature of laws available to Plaintiff and the Class make use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since Defendants would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

86. UC San Diego Health and Does 1 through 50 are based in San Diego, California, and on information and belief, all managerial decisions emanate from there, the representations on Defendants' website originate from there, Defendants' misrepresentations originated from California, and therefore application of California law to the Nationwide Class is appropriate.

87. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant

laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

88. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

89. Unless a Class-wide injunction is issued, Defendants may continue in its failure to properly secure the Sensitive Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

90. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

91. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and the Class Members to exercise due care in collecting, storing, using, and safeguarding their Sensitive Information;
b. Whether Defendants breached a legal duty to Plaintiff and the Class Members to exercise due care in collecting, storing, using, and safeguarding their Sensitive Information;
c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards

relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Class Members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

COUNT I

Negligence
(actionable through Gov. Code §§ 815.2 and 820)
(On Behalf of Plaintiff and the Class)

92. Plaintiff restates and realleges Paragraphs 1 through 91 as if fully set forth herein.

93. As a condition of receiving services or employment, Plaintiff and Class Members were obligated to provide Defendants, directly or indirectly, with their Sensitive Information.

94. Plaintiff and the Class Members entrusted their Sensitive Information to Defendants with the understanding that Defendants would safeguard their information.

95. Defendants had full knowledge of the sensitivity of the Sensitive Information and the types of harm that Plaintiff and Class Members could and would suffer if the Sensitive Information were wrongfully disclosed.

96. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized

parties. This duty includes, among other things, designing, maintaining, and testing its security protocols to ensure that Sensitive Information in their possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on relevant cybersecurity measures.

97. Defendants also owed a duty under various statutes. For example, Section 5 of the 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 UC San Diego Health, of failing to use reasonable measures to protect Sensitive Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

98. Defendants' violated Section 5 of the FTC Act by failing to use reasonable measures to protect patients' Sensitive Information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

99. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

100. 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 the Class.

101. Likewise, HIPAA privacy laws were enacted precisely with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient´s finances or reputation.

102. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

103. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

104. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew of or should have known of the inherent risks in collecting and storing the highly valuable Sensitive Information of Plaintiff and the Class, the critical importance of providing adequate security of that Sensitive Information, the current cyber scams being perpetrated, and that it had inadequate employee training and education and IT security protocols in place to secure the Sensitive Information of Plaintiff and the Class.

105. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decision not to comply with HIPAA and industry standards for the safekeeping and encrypted authorized disclosure of the Sensitive Information of Plaintiff and Class Members.

106. Plaintiff and the Class Members had no ability to protect their Sensitive Information that was in Defendants' possession.

107. Defendants were in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

108. Defendants had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiff and Class Members' Sensitive Information.

109. Defendants have admitted that Plaintiff' and Class Members' Sensitive Information was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

110. Defendants, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding the Plaintiff' and Class Members' Sensitive Information while it was in Defendants' possession or control.

111. Defendants improperly and inadequately safeguarded Plaintiff' and Class Members' Sensitive Information in deviation of standard industry rules, regulations and practices at the time of the Data Breach.

112. Defendants, through their actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' Sensitive Information.

113. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

114. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff' and Class Members' Sensitive Information would not have been compromised.

115. There is a temporal and close causal connection between Defendants' failure to implement security measures to protect the Sensitive Information and the harm suffered, or risk of imminent harm suffered, by Plaintiff and the Class.

116. As a result of Defendants' negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; present and continuing risk of identity theft and fraud and the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

COUNT II

Invasion of Privacy
(actionable through Gov. Code §§ 815.2 and 820)
(On Behalf of Plaintiff and the Class)

117. Plaintiff restates and realleges paragraph 1 through 91 as if fully set forth herein.

118. Plaintiff and Class Members had a legitimate expectation of privacy with respect to their Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

119. Defendants owed a duty to patients in its network, including Plaintiff and Class Members, to keep their Sensitive Information confidential.

120. The unauthorized release of Sensitive Information, especially the type related to personal health information, is highly offensive to a reasonable person.

121. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Sensitive Information to Defendants as part of their use of Defendants' services or employment with Defendants, but privately, with the intention that the Sensitive Information would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

122. The Data Breach constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

123. Defendants acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

124. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

125. As a proximate result of Defendants' acts and omissions, Plaintiff and Class Members' Sensitive Information was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

126. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Sensitive Information maintained by Defendants can be viewed, distributed, and used by unauthorized persons.

127. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT III

Breach of Implied Contract
(actionable through Gov. Code §§ 815.2 and 820)
(On Behalf of Plaintiff and the Class)

128. Plaintiff restates and realleges paragraphs 1 through 91 as if fully set forth herein.

129. Plaintiff and Class Members were required to provide their Sensitive Information, including their names, Social Security numbers, addresses, medical record numbers, dates of birth, telephone numbers, email addresses, and various health related information to Defendants as a condition of their use of Defendants' services.

130. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendants in exchange for services, along with Defendants' promise to protect their health information and other Sensitive Information from unauthorized disclosure.

131. In their written privacy policies, UC San Diego Health expressly promised Plaintiff and Class Members that it would only disclose protected health information and other Sensitive Information under certain circumstances, none of which relate to the Data Breach.

132. Defendants promised to comply with HIPAA standards and to make sure that Plaintiff's and Class Members' health information and other Sensitive Information would remain protected.

133. Implicit in the agreement between Plaintiff and Class Members and the Defendants to provide protected health information and other Sensitive Information, was Defendants' obligation to: (a) use such Sensitive Information for business purposes only; (b) take reasonable steps to safeguard that Sensitive Information; (c) prevent unauthorized disclosures of the Sensitive Information; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information; (e) reasonably safeguard and protect the Sensitive Information of Plaintiff and Class Members from unauthorized disclosure or uses; and (f) retain the Sensitive Information only under conditions that kept such information secure and confidential.

134. Without such implied contracts, Plaintiff and Class Members would not have provided their Sensitive Information to Defendants.

135. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendants. However, Defendants did not.

136. Defendants breached the implied contracts with Plaintiff and Class Members by failing to:

a. reasonably safeguard and protect Plaintiff's and Class Members' Sensitive Information, which was compromised as a result of the Data Breach;
b. comply with its promise to abide by HIPAA;
c. ensure the confidentiality and integrity of electronic protected health information that Defendants created, received,

maintained, and transmitted in violation of 45 C.F.R 164.306(a)(1);

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

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

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

g. protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R 164.306(a)(2).

137. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial and medical accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months if not years to discover and detect.

COUNT IV

Unjust Enrichment
(actionable through Gov. Code §§ 815.2 and 820)
(On Behalf of Plaintiff and the Class)

138. Plaintiff restates and realleges paragraphs 1 through 91 as if fully set forth herein.

139. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and in so doing provided Defendants with their Sensitive Information. In exchange, Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their Sensitive Information protected with adequate data security.

140. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Sensitive Information of Plaintiff and Class Members for business purposes.

141. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendants' network and the administrative costs of data management and security.

142. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

143. Defendants failed to secure Plaintiff's and Class Members' Sensitive Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

144. Defendants acquired the Sensitive Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

145. If Plaintiff and Class Members knew that Defendants had not reasonably secured their Sensitive Information, they would not have agreed to Defendants' services.

146. Plaintiff and Class Members have no adequate remedy at law.

147. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Sensitive Information is used; (c) the compromise, publication, and/or theft of their Sensitive Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Sensitive Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity 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 identity theft; (f) the continued risk to their Sensitive Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Sensitive Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

148. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

149. Defendants 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, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

COUNT V

Breach of Fiduciary Duty
(actionable through Gov. Code §§ 815.2 and 820)
(On Behalf of Plaintiff and the Class)

150. Plaintiff restates and realleges paragraphs 1 through 91 as if fully set forth herein.

151. In light of their special relationship, Defendants have become the guardian of Plaintiff' and Class Member's Sensitive Information. Defendants have become a fiduciary, created by their undertaking and guardianship of patients' Sensitive Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members. This duty included the obligation to safeguard Plaintiff's and Class Members' Sensitive Information and to timely notify them in the event of a data breach.

152. Defendants has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship. Defendants breached its fiduciary duties owed to Plaintiff and Class Members by failing to:

a. properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and Class Members' protected health information and other Sensitive Information;
b. timely notify and/or warn Plaintiff and Class Members of the Data Breach;
c. ensure the confidentiality and integrity of electronic protected health information Defendants created, received, maintained, and transmitted, in violation of 45 C.F.R 164.306(a)(1);
d. implement technical policies and procedures to limit access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R 164.312(a)(1);
e. implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R 164.308(a)(1);
f. identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R 164.308(a)(6)(ii);
g. protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R 164.306(a)(2);
h. protect against any 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);
i. ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R 164.306(a)(94);

j. prevent the improper use and disclosure of protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R 164.502, *et seq.*;

k. effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R 164.530(b) and 45 C.F.R 164.308(a)(5);

l. design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R 164.530(c); and

m. otherwise failing to safeguard Plaintiff's and Class Members' Sensitive Information.

153. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Sensitive Information is used; (c) the compromise, publication, and/or theft of their Sensitive Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (e) lost opportunity costs associated with the effort expended and the loss of productivity 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 identity theft; (f) the continued risk to their Sensitive

Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect patients' Sensitive Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

154. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI

Breach of Confidence
(actionable through Gov. Code §§ 815.2 and 820)
(On Behalf of Plaintiff and the Class)

155. Plaintiff restates and realleges paragraphs 1 through 91 as if fully set forth herein.

156. At all times during Plaintiff's and Class Members' interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Sensitive Information that Plaintiff and Class Members provided to Defendants.

157. As alleged herein and above, Defendants' relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Sensitive Information would be collected, stored, and protected in confidence, and would not be disclosed the unauthorized third parties.

158. Plaintiff and Class Members provided their respective Sensitive Information to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the Sensitive Information to be disseminated to any unauthorized parties.

159. Plaintiff and Class Members also provided their Sensitive Information to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that Sensitive Information from unauthorized disclosure, such as following basic principles of protecting its networks and data systems, including employees' email accounts.

160. Defendants voluntarily received in confidence Plaintiff's and Class Members' Sensitive Information with the understanding that the Sensitive Information would not be disclosed or disseminated to the public or any unauthorized third parties.

161. Due to Defendants' failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class Members' Sensitive Information, Plaintiff's and Class Members' Sensitive Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

162. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff and Class Members have suffered damages.

163. But for Defendants' disclosure of Plaintiff's and Class Members' Sensitive Information in violation of the parties' understanding of confidence, their Sensitive Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft

of Plaintiff's and Class Members' Sensitive Information, as well as the resulting damages.

164. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class Members' Sensitive Information. Defendants knew their computer systems and technologies for accepting and securing Plaintiff's and Class Members' Sensitive Information had numerous security and other vulnerabilities that placed Plaintiff's and Class Members' Sensitive Information in jeopardy.

165. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their Sensitive Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (d) lost opportunity costs associated with effort expended and the loss of productivity 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 identity theft; (e) the continued risk to their Sensitive Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Sensitive Information in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (g) the diminished value of Defendants' services they received.

COUNT VII

Violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq*.
(On Behalf of Plaintiff and the California Subclass)

166. Plaintiff restates and realleges paragraphs 1 through 91 as if fully set forth herein.

167. Defendants are providers of healthcare within the meaning of Civil Code § 56.06(a) and maintain medical information as defined by Civil Code § 56.05.

168. Plaintiff and the members of the California Subclass are patients of Defendants, as defined in Civil Code § 56.05(k).

169. Defendants maintain personal medical information of Plaintiff and the California Subclass.

170. Defendants negligently created, maintained, preserved, stored, and then exposed Plaintiff's and the California Subclass's individual identifiable "medical information," within the meaning of Civil Code § 56.05(j), including treatment information.

171. Defendants negligently created, maintained, preserved, stored, and released Plaintiff's and the California Subclass's medical information in violation of Civil Code section 56.101, subd. (a).

172. As a result of this negligence, Plaintiff's and the California Subclass's information was stolen and viewed by unauthorized third parties in the Data Breach.

173. Because Civil Code § 56.101 allows for the remedies and penalties provided under Civil Code § 56.36(b), Plaintiff, individually and for each member of the California Subclass, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code §56.36(b)(1),

and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2) and damages provided by the common law.

COUNT VIII

Violation of the California Consumer Privacy Act,
Cal. Civ. Code § 1798.100, *et seq*.
(On Behalf of Plaintiff and the California Subclass)

174. Plaintiff restates and realleges paragraphs 1 through 91 as if fully set forth herein.

175. Plaintiff and the California Subclass members are "consumer[s]" as that term is defined in Cal. Civ. Code § 1798.140(g).

176. Defendants are a "business" as that term is defined in Cal. Civ. Code. § 1798.140(c). Although the Regents are a non-profit entity, UC San Diego Health is a provider that generates profit for the Regents. Defendants collect consumers' (including Plaintiff's and California Subclass members') personal information and determine the purposes and means of the processing of this personal information (e.g., they design the systems that process and store consumers' personal information). Defendants annually receive for commercial purposes or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers.

177. Plaintiff and California Subclass members' PII is "nonencrypted and nonredacted personal information" as that term is used in Cal. Civ. Code § 1798.150(a)(1). At a minimum, this PII included the individual's first name or first initial and last name, in combination with Social Security numbers, bank account, and unique identification numbers issued on government documents (e.g., driver's license and passport numbers).

178. The Data Breach constitutes "an unauthorized access and exfiltration, theft, or disclosure" pursuant to Cal. Civ. Code § 1798.150(a)(1).

179. Under the CCPA, Defendants had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the Plaintiff's and California Subclass members' PII to protect said PII.

180. Defendants breached the duty it owed to Plaintiff Jackson and California Subclass members by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiff Jackson and California Subclass members; (b) detect the Data Breach while it was ongoing; and (c) maintain security systems consistent with industry standards.

181. Defendants' breach of the duty it owed to Plaintiff and California Subclass members described above was the direct and proximate cause of the Data Breach. As a result, Plaintiff and California Subclass members suffered damages, as described above and as will be proven at trial.

182. Plaintiff seeks injunctive relief in the form of an order enjoining Defendants from continuing the practices that constituted its breach of the duty owed to Plaintiff and California Subclass members as described above.

183. Plaintiff also seeks actual damages, and all other forms of relief available under the CCPA.

184. Contemporaneously with filing this Complaint, and on or about September 22, 2021, Plaintiff sent Defendant via certified mail the 30-day notice letter as required under Civil Code section 1798.150, subd. (b). Plaintiff and the Class members reserve the right to amend this Complaint

as of right to seek statutory damages and relief following the expiration of the 30-day period.

Prayer for Relief

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, request judgment against the Defendants and that the Court grant the following:

A. An order certifying the Nationwide Class and California Subclass as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

B. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and Class Members' Sensitive Information;

C. An award of compensatory and statutory damages, in an amount to be determined;

D. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

E. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

F. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: September 22, 2021

Respectfully submitted,

s/ Gayle M. Blatt

Gayle M. Blatt, SBN 122048
gmb@cglaw.com
P. Camille Guerra, SBN 326546
camille@cglaw.com
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232

Melissa R. Emert (*pro hac vice forthcoming)*
Gary S. Graifman (*pro hac vice forthcoming*)
KANTROWITZ GOLDHAMER & GRAIFMAN, P.C.
747 Chestnut Ridge Road
Chestnut Ridge, New York 10977
Tel: (845) 356-2570
Fax: (845) 356-4335
memert@kgglaw.com
ggraifman@kgglaw.com

Attorneys for Plaintiff Richard Hartley

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

RICHARD HARTLEY, on behalf of himself and all others similarly situated

(b) County of Residence of First Listed Plaintiff San Diego
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Casey Gerry Schenk Francavilla Blatt & Penfiled LLP
110 Laurel St., San Diego, CA 92101, (619) 238-1811

DEFENDANTS

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA d/b/a UC SAN DIEGO HEALTH, a public entity, and DOES

County of Residence of First Listed Defendant San Diego
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

'21CV1668 H KSC

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☑ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

fth

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 422 Appeal 28 USC 158	☐ 375 False Claims Act
☐ 120 Marine	☐ 310 Airplane	☐ 365 Personal Injury - Product Liability	☐ 690 Other	☐ 423 Withdrawal 28 USC 157	☐ 376 Qui Tam (31 USC 3729(a))
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	☐ 400 State Reapportionment
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability		☐ 820 Copyrights	☐ 410 Antitrust
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	☐ 830 Patent	☐ 430 Banks and Banking
☐ 151 Medicare Act	☐ 340 Marine	☐ 370 Other Fraud	☐ 710 Fair Labor Standards Act	☐ 835 Patent - Abbreviated New Drug Application	☐ 450 Commerce
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 720 Labor/Management Relations	☐ 840 Trademark	☐ 460 Deportation
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 740 Railway Labor Act	☐ 880 Defend Trade Secrets Act of 2016	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	☐ 751 Family and Medical Leave Act	SOCIAL SECURITY	☐ 480 Consumer Credit (15 USC 1681 or 1692)
☐ 190 Other Contract	☐ 360 Other Personal Injury		☐ 790 Other Labor Litigation	☐ 861 HIA (1395ff)	☐ 485 Telephone Consumer Protection Act
☐ 195 Contract Product Liability	☐ 362 Personal Injury - Medical Malpractice		☐ 791 Employee Retirement Income Security Act	☐ 862 Black Lung (923)	☐ 490 Cable/Sat TV
☐ 196 Franchise				☐ 863 DIWC/DIWW (405(g))	☐ 850 Securities/Commodities/ Exchange
				☐ 864 SSID Title XVI	☒ 890 Other Statutory Actions
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS		☐ 865 RSI (405(g))	☐ 891 Agricultural Acts
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	Habeas Corpus:			☐ 893 Environmental Matters
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee		FEDERAL TAX SUITS	☐ 895 Freedom of Information Act
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence		☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 896 Arbitration
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General		☐ 871 IRS—Third Party 26 USC 7609	☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 535 Death Penalty	IMMIGRATION		☐ 950 Constitutionality of State Statutes
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	Other:	☐ 462 Naturalization Application		
	☐ 448 Education	☐ 540 Mandamus & Other	☐ 465 Other Immigration Actions		
		☐ 550 Civil Rights			
		☐ 555 Prison Condition			
		☐ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District *(specify)*
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***: 28 U.S.C. 1332

Brief description of cause: Class action stemming from data theft at UCSD

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions):*

JUDGE Hon. Roger T.Benitez DOCKET NUMBER 3:21-cv-01641-BEN-JLB

DATE
September 22, 2021

SIGNATURE OF ATTORNEY OF RECORD
s/ Gayle M. Blatt

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.