

1 Jason S. Hartley (SBN 192514)
2 **HARTLEY LLP**
3 101 West Broadway, Suite 820
4 San Diego, California 92101
5 Tel: 619-400-5822
6 *hartley@hartleyllp.com*

7 Norman E. Siegel
8 J. Austin Moore
9 **STUEVE SIEGEL HANSON LLP**
10 460 Nichols Road, Suite 200
11 Kansas City, Missouri 64112
12 Tel: 816-714-7100
13 *siegel@stuevesiegel.com*
14 *moore@stuevesiegel.com*

15 **UNITED STATES DISTRICT COURT**
16 **SOUTHERN DISTRICT OF CALIFORNIA**

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

20 Plaintiff,

21 v.

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

25 Defendant.

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

CLASS ACTION COMPLAINT

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

DEMAND FOR JURY TRIAL

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

7 **NATURE OF THE ACTION**

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

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

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

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

4 **PARTIES**

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

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

18 **JURISDICTION AND VENUE**

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

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

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

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

4 **FACTUAL ALLEGATIONS**

5 ***UC San Diego Health's Privacy Practices***

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

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

23 11. Given the amount and sensitive nature of the data it collects, UC San
24 Diego Health maintains a "Notice of Privacy Practices" which describes how
25 medical information about its patients will be used and disclosed.¹ UC San Diego
26 Health represents that "All new patients are provided a copy of the Notice of
27

28 ¹ <https://health.ucsd.edu/hipaa/Pages/hipaa.aspx> (last visited September 20, 2021).

1 Privacy Practices and will be asked to sign a form indicating they have read and
2 reviewed this notice.”²

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

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

17 ***The Data Breach***

18 14. Contrary to its representations, on December 2, 2020, hackers were
19 able to access the email accounts of UC San Diego Health’s employees through a
20 successful “phishing” attempt. Phishing is the practice of sending fraudulent emails,
21 oftentimes targeting a company’s employees, purporting to be from a reputable
22

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

24 ³ <https://health.ucsd.edu/hipaa/Pages/hipaa.aspx> (last visited September 20, 2021).

25 ⁴ *Id.*

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

27 ⁶
28 [https://health.ucsd.edu/patients/yourhospitalstay/Documents/Patient%20Rights%
20and%20Responsibilities%20Handout.pdf](https://health.ucsd.edu/patients/yourhospitalstay/Documents/Patient%20Rights%20and%20Responsibilities%20Handout.pdf) (last visited September 20, 2021).

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

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

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

19 ***The Data Breach was Preventable***

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

26 _____
27 ⁷ <https://health.ucsd.edu/data-security/Pages/default.aspx> (last visited September 20,
2021).

28 ⁸ *Id.*

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

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

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

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

21 21. In December 2017, UC San Diego Health learned that an unauthorized
22 third party gained access to one of its business associates' medical transcription
23 platforms containing names, dates of birth, ages, genders, medical record numbers,
24 and clinical information for a number of patients. Well over six months later, UC
25 San Diego Health informed affected individuals of the breach, noting that “[o]ne of
26

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

1 UC San Diego Health’s top priorities is to protect and maintain the confidentiality of
2 patient information.”¹⁰

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

8 23. Phishing attacks in particular have been on the rise. According to the
9 Federal Bureau of Investigation (FBI), phishing was the most common type of
10 cybercrime in 2020 and phishing incidents nearly doubled in frequency between
11 2019 and 2020.¹³ According to Verizon’s 2021 Data Breach Investigations Report
12 (DBIR), phishing is the top “action variety” seen in breaches in the last year and
13 43% of breaches involved phishing and/or pretexting.¹⁴

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

19 _____
20 ¹⁰ https://oag.ca.gov/system/files/ACID_PRINTERPROOFS_ACID_20180627_UCS_D501_R1_1.pdf (last visited September 20, 2021).

21 ¹¹ <https://www.hipaajournal.com/healthcare-data-breach-statistics/> (last visited
22 September 20, 2021).

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

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

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

27 ¹⁵ [https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20Activity Targeting the Healthcare and Public Health S
28 ector.pdf](https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20Activity%20Targeting%20the%20Healthcare%20and%20Public%20Health%20Sector.pdf) (last visited September 20, 2021).

1 Department of Health and Human Services (HHS), and the FBI issued the advisory
2 to warn healthcare providers to take “timely and reasonable precautions to protect
3 their networks from these threats.”¹⁶

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

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

19 27. Employee education provides the easiest method to assist employees in
20 properly identifying fraudulent e-mails and prevent unauthorized access of sensitive
21 internal information. According to September 2020 guidance from CISA,
22 organizations housing sensitive data should “[i]mplement a cybersecurity user
23 awareness and training program that includes guidance on how to identify and report
24 suspicious activity” and conduct “organization-wide phishing tests to gauge user
25
26
27

28 ¹⁶ *Id.*

1 awareness and reinforce the importance of identifying potentially malicious
2 emails.”¹⁷

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

15 29. Additionally, because the goal of many phishing attempts is to gain an
16 employee’s login credentials in order to access a company’s network, there are
17 industry-standard measures that companies can implement to greatly reduce
18 unauthorized access, even if a phishing attempt is successful. For example, multi-
19 factor authentication is a security system that requires more than one method of
20 authentication from independent categories of credentials to verify the user’s
21 identity for a login. This could include entering a code from the user’s smartphone,
22 answering a security question, or providing a biometric indicator such as a
23 fingerprint or facial recognition—in addition to entering a username and password.
24 Thus, even if hackers obtain an employee’s username and password, access to the
25

26
27 ¹⁷ [https://www.cisa.gov/sites/default/files/publications/CISA_MS-
ISAC_Ransomware%20Guide_S508C_.pdf](https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf) (last visited September 20, 2021).

28 ¹⁸ *Id.*

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

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

14 31. Network segmentation is commonly used in conjunction with the
15 principle of least privilege (POLP), which is a security practice that limits
16 employees' privileges to the minimum necessary to perform the job or task. In an IT
17 environment, adhering to POLP reduces the risk of hackers gaining access to critical
18 systems or sensitive data by compromising a low-level user account, device, or
19 application.¹⁹ In an example given by security software provider Digital Guardian,
20 "an employee whose job is to enter info into a database only needs the ability to add
21 records to that database. If malware infects that employee's computer or if the
22 employee clicks a link in a phishing email, the malicious attack is limited to making
23 database entries. If that employee has root access privileges, however, the infection
24 can spread system-wide."²⁰ This is why approximately 67% of targeted malware and
25

26
27 ¹⁹ [https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-
information-security-and-compliance](https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance) (last visited September 20, 2021).

28 ²⁰ *Id.*

1 phishing attacks are directed at individual contributors and lower-level management
2 personnel.²¹

3 32. In addition to addressing “phishing” attempts, the CISA guidance
4 encourages organizations to prevent unauthorized access by:

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

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

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

26 ²¹ [https://healthitsecurity.com/news/pharmaceutical-companies-most-targeted-](https://healthitsecurity.com/news/pharmaceutical-companies-most-targeted-industry-by-cybercriminals)
27 [industry-by-cybercriminals](https://healthitsecurity.com/news/pharmaceutical-companies-most-targeted-industry-by-cybercriminals) (last visited September 20, 2020).

28 ²² [CISA Guide](#) at 4.

²³ *Id.* at 5.

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

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

10 *Allegations Relating to Plaintiff Denise Menezes*

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

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

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

21 39. In September 2021, Ms. Menezes received a notification letter from UC
22 San Diego Health informing her that she was a victim of the Data Breach. The letter
23 stated: “As previously disclosed July 27, 2021, UC San Diego Health recently
24 identified and responded to a security matter involving unauthorized access to some
25 employee email accounts.” The letter further stated: “We determined September 1,
26 2021 that emails or attachments containing some of your personal information were
27 accessed and/or acquired by the unauthorized actor between December 2, 2020 and
28 April 8, 2021, including the following: full name; claims information (date and cost

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

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

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

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

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

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

10 44. UC San Diego Health is a healthcare provider covered by the Health
11 Insurance Portability and Accountability Act of 1996 (“HIPAA”) (*see* 45 C.F.R. §
12 160.102) and as such is required to comply with the HIPAA Privacy Rule and
13 Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E (“Standards for
14 Privacy of Individually Identifiable Health Information”), and Security Rule
15 (“Security Standards for the Protection of Electronic Protected Health
16 Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

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

22 46. HIPAA limits the permissible uses of “protected health information”
23 and prohibits unauthorized disclosures of “protected health information.”²⁴

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

26
27 _____
28 ²⁴ 45 C.F.R. § 164.502.

²⁵ 45 C.F.R. § 164.530(c)(1).

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

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

- 8 a. Maintain an adequate data security system to reduce the risk of data
9 breaches and cyberattacks;
- 10 b. Adequately protect the PII of its patients and employees;
- 11 c. Ensure the confidentiality and integrity of electronically protected
12 health information created, received, maintained, or transmitted, in
13 violation of 45 C.F.R. § 164.306(a)(1);
- 14 d. Implement technical policies and procedures for electronic information
15 systems that maintain electronically protected health information to
16 allow access only to those persons or software programs that have been
17 granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);
- 18 e. Implement adequate policies and procedures to prevent, detect, contain,
19 and correct security violations, in violation of 45 C.F.R. §
20 164.308(a)(1)(i);
- 21 f. Implement adequate procedures to review records of information
22 system activity regularly, such as audit logs, access reports, and
23 security incident tracking reports, in violation of 45 C.F.R. §
24 164.308(a)(1)(ii)(D);
- 25 g. Protect against reasonably anticipated uses or disclosures of electronic
26 protected health information that are not permitted under the privacy
27 rules regarding individually identifiable health information, in violation
28 of 45 C.F.R. § 164.306(a)(3);
- h. Ensure compliance with the electronically protected health information
security standard rules by their workforces, in violation of 45 C.F.R. §
164.306(a)(4); and/or
- i. Train all members of their workforces effectively on the policies and
procedures with respect to protected health information as necessary

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

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

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

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

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

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

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

²⁹ *Id.*

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

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

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

17 *The Impact of the Data Breach on Victims*

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

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

26 _____
27 ³⁰ FTC, *Start With Security*, *supra* note 41.

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

1 combine a patient number with a false provider number and file made-up claims
2 with insurers.”³²

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

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

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

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

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

26 ³⁵ <https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web> (last visited September 20,
27 2021).
28

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

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

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

21 62. Exacerbating the problem, victims of medical identity theft oftentimes
22 struggle to resolve the issue because HIPAA regulations require the victim to be
23 personally involved in the resolution of the crime.⁴⁰ In some cases, victims may not
24

25 ³⁶ https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65
26 (“Ponemon Study”) (last visited September 20, 2021).

27 ³⁷ *Id.* at 9.

28 ³⁸ *Id.* at 2.

³⁹ *Id.* at 14.

⁴⁰ *Id.* at 1.

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

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

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

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

26 ⁴¹ *Id.*

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

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

1 further theft or errors in healthcare records that could jeopardize medical treatments
2 and diagnosis.”⁴⁴

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

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

21 67. Given the amount of time hackers had access to UC San Diego
22 Health’s systems, many victims of the Data Breach have likely already experienced
23

24 ⁴⁴ [Ponemon Study](#) at 1.

25 ⁴⁵ <https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/>
(last visited September 20, 2021).

26 ⁴⁶ *Id.*

27 ⁴⁷ [https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-
data-perfcon](https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon) (last visited September 20, 2021).

28 ⁴⁸ *Id.*

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

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

- 10 • 75% of respondents reported feeling severely distressed
- 11 • 67% reported anxiety
- 12 • 66% reported feelings of fear related to personal financial safety
- 13 • 37% reported fearing for the financial safety of family members
- 14 • 24% reported fear for their physical safety
- 15 • 15.2% reported a relationship ended or was severely and negatively
16 impacted by the identity theft
- 17 • 7% reported feeling suicidal.⁴⁹

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

- 21 • 48.3% of respondents reported sleep disturbances
- 22 • 37.1% reported an inability to concentrate / lack of focus
- 23 • 28.7% reported they were unable to go to work because of physical
24 symptoms
- 25 • 23.1% reported new physical illnesses (aches and pains, heart
26 palpitations, sweating, stomach issues)

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

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

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

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

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

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

⁵⁰ *Id.*

- 1 f. costs associated with purchasing credit monitoring, credit freezes, and
identity theft protection services;
- 2 g. unauthorized charges and loss of use of and access to their financial and
3 investment account funds and costs associated with inability to obtain
4 money from their accounts or being limited in the amount of money
5 they were permitted to obtain from their accounts, including missed
payments on bills and loans, late charges and fees, and adverse effects
6 on their credit;
- 7 h. lowered credit scores resulting from credit inquiries following
8 fraudulent activities;
- 9 i. costs associated with time spent and the loss of productivity or the
10 enjoyment of one's life from taking time to address and attempt to
11 mitigate and address the actual and future consequences of the Data
Breach, including searching for fraudulent activity, imposing
12 withdrawal and purchase limits on compromised accounts, and the
13 stress, nuisance, and annoyance of dealing with the repercussions of the
Data Breach; and
- 14 j. the continued, imminent, and certainly impending injury flowing from
15 potential fraud and identify theft posed by their PII being in the
16 possession of one or many unauthorized third parties.

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

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

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

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

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

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

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

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

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

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

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

19 CLASS ACTION ALLEGATIONS

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

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

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

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

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

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

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

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

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

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

- 26 a. Whether Defendant violated § 1798.150 of the CCPA;
27
28

- b. Whether Defendant owed Plaintiff and class members a duty to implement and maintain reasonable security procedures and practices to protect their PII;
- c. Whether Defendant breached an express or implied contract with Plaintiff and class members, including whether Defendant breached an agreement with Plaintiff and class members to keep their PII confidential;
- d. Whether Defendant received a benefit without proper restitution making it unjust for Defendant to retain the benefit without commensurate compensation;
- e. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiff's and class members' PII;
- f. Whether Defendant Plaintiff's its duty to implement reasonable security systems to protect Plaintiff's and class members' PII;
- g. Whether Defendant's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and class members;
- h. Whether Defendant adequately addressed and fixed the vulnerabilities that enabled the Data Breach;
- i. Whether Plaintiff and class members are entitled to credit monitoring and other injunctive relief;
- j. Whether Defendant provided timely notice of the Data Breach to Plaintiff and class members; and,
- k. Whether class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

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

1 88. Superiority: A class action is superior to other available methods for the
2 fair and efficient adjudication of the controversy. Class treatment of common
3 questions of law and fact is superior to multiple individual actions or piecemeal
4 litigation. Absent a class action, most if not all class members would find the cost of
5 litigating their individual claims prohibitively high and have no effective remedy.
6 The prosecution of separate actions by individual class members would create a risk
7 of inconsistent or varying adjudications with respect to individual class members
8 and risk inconsistent treatment of claims arising from the same set of facts and
9 occurrences. Plaintiff knows of no difficulty likely to be encountered in the
10 maintenance of this action as a class action under Federal Rule of Civil Procedure
11 23.

12 **CLAIMS FOR RELIEF**

13 **COUNT I**

14 **Violation of the California Consumer Privacy Act of 2018 (“CCPA”)**
15 **Cal. Civ. Code § 1798.150**
 (On Behalf of the California Class)

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

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

25 91. Defendant violated § 1798.150 of the CCPA by failing to prevent
26 Plaintiff’s and class members’ nonencrypted PII from unauthorized access and
27 exfiltration, theft, or disclosure as a result of Defendant’s violations of its duty to
28

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

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

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

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

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

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

COUNT II

**Violation of California’s Confidentiality of Medical Information Act
 (“CMIA”)**

**Cal. Civ. Code § 56, *et seq.*
 (On Behalf of the California Class)**

1
2
3
4
5 97. Plaintiff repeats and realleges every allegation set forth in the preceding
6 paragraphs.

7 98. Defendant is a “provider of healthcare” pursuant to Cal. Civ. Code §
8 56.06, and is subject to the requirements of the CMIA, Cal. Civ. Code §§ 56.10(a)
9 and (e), 56.36, 56.101.

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

12 100. Defendant disclosed “medical information,” as defined in CMIA, Cal.
13 Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in
14 violation of Cal. Civ. Code § 56.10(a). The disclosure of information to
15 unauthorized individuals in the Data Breach occurred when an employee or
16 employees of Defendant affirmatively granted access to confidential emails,
17 attachments, and the PII contained therein, to unauthorized individuals by
18 responding to their phishing attempts. This disclosure was exacerbated by
19 Defendant’s previous failure to implement reasonable and adequate data security
20 measures and protocols to protect Plaintiff’s and class members’ PII.

21 101. Defendant’s negligent failure to maintain, preserve, store, abandon,
22 destroy, and/or dispose of Plaintiff and class members’ medical information in a
23 manner that preserved the confidentiality of the information contained therein
24 violated the CMIA, Cal. Civ. Code §§ 56.06 and 56.101(a). By Defendant’s own
25 admission, confidential medical information contained in unencrypted emails and
26 attachments has been accessed and viewed by an unauthorized third party or parties.
27 Accordingly, Defendant’s systems and protocols did not protect and preserve the
28

1 integrity of electronic medical information in violation of the CMIA, Cal. Civ. Code
2 § 56.101.

3 102. Plaintiff and class members were injured and have suffered damages, as
4 described above, from Defendant’s illegal disclosure and negligent release of their
5 medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and
6 therefore seek relief under Cal. Civ. Code §§ 56.35 and 56.36, including actual
7 damages, nominal statutory damages of \$1,000, punitive damages of \$3,000,
8 injunctive relief, and attorneys’ fees, expenses and costs.

9
10 **COUNT III**

11 **Violation of California’s Unfair Competition Law (“UCL”)**
12 **Cal. Bus. Prof. Code § 17200, et seq.**
(On Behalf of the California Class)

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

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

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

18 106. Defendant’s “unfair” acts and practices include:

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

- b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in state and federal laws including the FTC Act, 15 U.S.C. § 45; HIPAA, 42 U.S.C. § 1302d, *et seq.*; the CCPA, Cal. Civ. Code § 1798.150; the CMIA, Cal. Civ. Code § 56, *et seq.*; and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.
- c. Defendant's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's grossly inadequate security, consumers could not have reasonably avoided the harms that Defendant caused.
- d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

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

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

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' PII;

- 1 d. Misrepresenting that it would protect the privacy and confidentiality
2 of Plaintiff and Class members' PII, including by implementing and
3 maintaining reasonable security measures;
- 4 e. Misrepresenting that it would comply with common law and
5 statutory duties pertaining to the security and privacy of Plaintiff
6 and Class members' PII;
- 7 f. Omitting, suppressing, and concealing the material fact that it did
8 not reasonably or adequately secure Plaintiff and Class members'
9 PII; and
- 10 g. Omitting, suppressing, and concealing the material fact that it did
11 not comply with common law and statutory duties pertaining to the
12 security and privacy of Plaintiff and class members' PII.

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

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

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

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

1 unfair, unlawful, and fraudulent business practices or use of their PII; declaratory
2 relief; reasonable attorneys' fees and costs under California Code of Civil Procedure
3 § 1021.5; injunctive relief; and other appropriate equitable relief.

4
5 **COUNT IV**

6 **Negligence**

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

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

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

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

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

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

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

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

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

- 6 a. Failing to exercise reasonable care and implement adequate security
7 systems, protocols, and practices sufficient to protect the PII of
8 Plaintiff and class members;
- 9 b. Failing to comply with industry standard data security measures for
10 the healthcare industry leading up to the Data Breach;
- 11 c. Failing to comply with its own privacy policies;
- 12 d. Failing to comply with regulations protecting the PII at issue during
13 the period of the Data Breach;
- 14 e. Failing to adequately monitor, evaluate, and ensure the security of
15 Defendant's network and systems;
- 16 f. Failing to recognize in a timely manner that PII had been
17 compromised; and
- 18 g. Failing to timely and adequately disclose the Data Breach.

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

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

28

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

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

20 **COUNT V**

21 **Negligence *Per Se***

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

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

25 126. As a healthcare provider, Defendant is covered by HIPAA, 45 C.F.R. §
26 160.102, and is therefore obligated to comply with all rules and regulations under 45
27 C.F.R. Parts 160 and 164.

1 127. 45 C.F.R. Part 164 governs “Security and Privacy,” with Subpart A
2 providing “General Provisions,” Subpart B regulating “Security Standards for the
3 Protection of Electronic Protected Health Information,” Subpart C providing
4 requirements for “Notification in the Case of Breach of Unsecured Protected Health
5 Information,” and Subpart E governing “Privacy of Individually Identifiable Health
6 Information.”

7 128. 45 C.F.R. § 164.104 states that the “standards, requirements, and
8 implementation specifications adopted under this part” apply to covered entities and
9 their business associates, such as Defendant.

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

15 130. 45 C.F.R. Sections 164.308 (Administrative safeguards), 164.310
16 (Physical safeguards), 164.312 (Technical safeguards), 164.314 (Organizational
17 requirements), and 164.316 (Policies and procedures and documentation
18 requirements) provide mandatory standards that all covered entities must adhere to.

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

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

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

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

7 134. HIPAA requires Defendant to “reasonably protect” confidential data
8 from “any intentional or unintentional use or disclosure” and to “have in place
9 appropriate administrative, technical, and physical safeguards to protect the privacy
10 of protected health information.” 45 C.F.R. § 164.530(c)(1). The confidential data at
11 issue in this case constitutes “protected health information” within the meaning of
12 HIPAA.

13 135. HIPAA further requires Defendant to disclose the unauthorized access
14 and theft of the PII to Plaintiff and class members “without unreasonable delay” so
15 that Plaintiff and class members can take appropriate measures to mitigate damages,
16 protect against adverse consequences, and detect misuse of their PII. See 45 C.F.R.
17 § 164.404.

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

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

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

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

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

1 as Defendant, of failing to use reasonable measures to protect PII. 15 U.S.C.
2 § 45(a)(1).

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

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

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

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

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

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

23
24 **COUNT VI**

25 **Breach of Contract**

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

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

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

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

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

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

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

23 **COUNT VII**

24 **Breach of Implied Contract**

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

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

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

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

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

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

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

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

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

28

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

10 **COUNT IX**

11 **Breach of Confidence**

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

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

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

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

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

26 173. As a direct and proximate result of Defendant's breach of confidence,
27 Plaintiff and class members suffered injury and sustained actual losses and damages
28

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

3 **COUNT X**

4 **Declaratory Judgment**
5 ***(On Behalf of the Nationwide Class)***

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

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

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

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

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

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

- 6
- 7 a. Engaging third-party security auditors/penetration testers as well as
8 internal security personnel to conduct testing, including simulated
9 attacks, penetration tests, and audits on Defendant's systems on a
10 periodic basis, and ordering Defendant to promptly correct any
11 problems or issues detected by such third-party security auditors;
 - 12 b. Engaging third-party security auditors and internal personnel to run
13 automated security monitoring;
 - 14 c. Auditing, testing, and training its security personnel regarding any
15 new or modified procedures;
 - 16 d. Encrypting PII and segmenting PII by, among other things, creating
17 firewalls and access controls so that if one area of Defendant's
18 systems is compromised, hackers cannot gain access to other
19 portions of its systems;
 - 20 e. Purging, deleting, and destroying in a reasonable and secure manner
21 PII not necessary to perform essential business functions;
 - 22 f. Conducting regular database scanning and security checks;
 - 23 g. Conducting regular employee education regarding best security
24 practices;
 - 25 h. Implementing multi-factor authentication and POLP to combat
26 system-wide cyberattacks; and
 - 27 i. Routinely and continually conducting internal training and
28 education to inform internal security personnel how to identify and
contain a breach when it occurs and what to do in response to a
breach.

1 **REQUEST FOR RELIEF**

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

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

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

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

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

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

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

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

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

24 **DEMAND FOR JURY TRIAL**

25 Plaintiff hereby demands a jury trial in the instant action.
26
27
28

1 Dated: September 20, 2021

2 /s/ Jason S. Hartley
3 Jason S. Hartley (SBN 192514)
4 **HARTLEY LLP**
5 101 West Broadway, Suite 820
6 San Diego, California 92101
7 Tel: 619-400-5822
8 *hartley@hartleyllp.com*

9 Norman E. Siegel*
10 J. Austin Moore*
11 **STUEVE SIEGEL HANSON LLP**
12 460 Nichols Road, Suite 200
13 Kansas City, Missouri 64112
14 Tel: 816-714-7100
15 *siegel@stuevesiegel.com*
16 *moore@stuevesiegel.com*
17 **Pro Hac Vice Forthcoming*

18
19
20
21
22
23
24
25
26
27
28
Counsel for Plaintiff and the Class

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

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

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

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

Jason S. Hartley, HARTLEY LLP, 101 W. Broadway, Ste. 820, San Diego, CA 92101 (619) 400-5822

DEFENDANTS

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

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

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

Attorneys (If Known)

'21CV1641 BEN JLB

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

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

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship: Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation.

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

Click here for: Nature of Suit Code Descriptions.

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

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 USC § 1332
Brief description of cause: Data breach

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 DOCKET NUMBER

DATE: September 20, 2021 SIGNATURE OF ATTORNEY OF RECORD: /s/ Jason S. Hartley

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 statute.
- 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.