Exhibit 4

BETSY C. MANIFOLD (182450)
RACHELE R. BYRD (190634)
MARISA C. LIVESAY (223247)
BRITTANY N. DEJONG (258766)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599
manifold@whafh.com
byrd@whafh.com
livesay@whafh.com
dejong@whafh.com

M. ANDERSON BERRY
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com

Attorneys for Plaintiff and the Proposed Class

[Additional Counsel Appear on Signature Page]

SUPERIOR COURT OF CALIFORNIA
IN AND FOR THE COUNTY OF SAN DIEGO

DACIA THOMAS, *individually and on behalf of all others similarly situated*,

Plaintiff,

v.

SAN DIEGO FAMILY CARE,

Defendant.

Case No. 37-2021-00026758-CU-BT-CTL

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Dacia Thomas ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this action against Defendant San Diego Family Care (hereinafter known as "SDFC" or "Defendant"), a California nonprofit corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach on SDFC's network that resulted in unauthorized access to the sensitive data of current and former SDFC patients and employees (the "Data Breach"). As a result of the Data Breach, Plaintiff and approximately 125,500 Class Members[1] suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

2. In addition, Plaintiff's and Class Members' sensitive personal information—which was entrusted to SDFC and its officials and agents—was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes names, Social Security numbers or other government identification numbers, financial account numbers, dates of birth, medical diagnosis or treatment information, health insurance information, and/or client identification numbers, and other protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") and PHI that Defendant SDFC collected and maintained (collectively the "Private Information").

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private

[1] *See Cases Currently Under Investigation*, Office for Civil Rights, U.S. DEPT. OF HEALTH AND HUMAN SERVICES, *available at:* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited June 18, 2021).

Information that SDFC collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific types of information was accessed.

5. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

6. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that SDFC collected and maintained is now in the hands of data thieves.

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

9. Plaintiff and Class Members may also incur out-of-pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. By her Complaint, Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

11. Plaintiff seeks remedies including, but not limited to, compensatory damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

12. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) intrusion into private affairs, (iii) breach of express contract, (iv) breach of implied contract, (v) breach of fiduciary duty, (vi) unjust enrichment, (vii) deprivation of rights possessed under the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq*., and (viii) deprivation of rights possessed under the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*., and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*.

JURISDICTION AND VENUE

13. This Court has jurisdiction over the causes of action asserted herein pursuant to the California Constitution, article VI, section 10, because this case is a cause not given by statute to other trial courts and pursuant to Cal. Code Civ. Proc. § 410.10 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on behalf of Plaintiff and Class Members pursuant to Cal. Code Civ. Proc. § 382. The amount in controversy exceeds the jurisdictional minimum of this Court. The amount in controversy as to the Plaintiff individually and each individual Class member does not exceed $75,000, including interest and any *pro rata* award of attorneys' fees, costs, and damages. This action is not removable.

14. This Court has personal jurisdiction over Defendant because it is located within and regularly conducts business in California.

15. Venue is proper in this Court pursuant to Cal. Bus. & Prof. Code § 17203 and Cal. Code of Civ. Proc. §§ 390 and 395.5 because Defendant regularly conducts business in the State of California and in San Diego County; Defendant has obtained PII and PHI in the transaction of

business in San Diego County, which has caused both Defendant's obligations and liability to arise in San Diego County; and Defendant's agent for service of process is located within San Diego County.

PARTIES

16. Plaintiff Dacia Thomas is, and at all times mentioned herein was, an individual citizen of the State of California residing in San Diego, California. Plaintiff Thomas was notified of the Data Breach and her Private Information being compromised upon receiving a data breach notice letter dated May 7, 2021.[2]

17. Defendant San Diego Family Care is a domestic nonprofit corporation organized under the laws of the State of California with its principal place of business located at 6973 Linda Vista Road, San Diego, CA 92111.

DEFENDANT'S BUSINESS

18. SDFC is a "culturally competent, affordable, fiscally responsible and accessible primary care agency serving San Diego County."[3]

19. SDFC, established in 1972, operates eight "health centers" throughout San Diego County as of 2021, and claims to provide over 115,000 healthcare appointments annually.[4]

20. Defendant SDFC provides healthcare services in the following areas: adult medicine, pediatrics, dental, mental health, prenatal, reproductive health, and teen services.[5]

21. On information and belief, in the ordinary course of rendering healthcare care services, SDFC requires patients and employees to provide sensitive personal and private information such as:

- Name, address, phone number and email address;
- Date of birth;

---

[2] *See* Exhibit A.
[3] *About SDFC*, SDFC, *available at:* https://sdfamilycare.org/about-sdfc/ (last visited June 18, 2021).
[4] *Id*.
[5] *See Our Services*, SDFC, *available at:* https://sdfamilycare.org/services/ (last visited June 18, 2021).

- Demographic information;
- Social Security number;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification;
- Employment information, and;
- Other information that may be deemed necessary to provide care.

22. Additionally, SDFC may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patients' health plan(s), close friends, and/or family members.

23. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

24. On information and belief, SDFC provides each of its patients, including Plaintiff and Class Members, with a HIPAA compliant notice titled, "Notice of Privacy Practices" (the "Privacy Notice") that explains how they handle patients' sensitive and confidential information.[6]

25. The Privacy Notice is posted on Defendant's website[7] and, upon information and belief, provided to each patient (including Plaintiff) prior to receiving treatment or services, and is provided to every patient upon request.

26. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, SDFC, promises to, among other things: keep patients' PHI private; inform patients of its legal duties and comply with laws protecting patients' health information; only use and release patients' health information for approved reasons; provide adequate notice to patients if their Private Information is disclosed without authorization;

---

[6] *See Privacy*, SDFC, *available at:* https://sdfamilycare.org/privacy/ (last visited June 18, 2021).
[7] *Id*.

and adhere to the terms outlined in the Privacy Notice.[8]

27. Defendant's Privacy Notice, provides, in relevant parts, the following:

> **THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW THIS NOTICE CAREFULLY.**
>
> **Summary of Rights and Obligations Concerning Health Information**
> San Diego Family Care is **committed to preserving the privacy and confidentiality of your health information**, which is required both by federal and state law. We are required by law to provide you with this notice of our legal duties, your rights, and our privacy practices, with respect to using and disclosing your health information that is created or retained by San Diego Family Care. Each time you visit us, we make a record of your visit. Typically, this record contains your symptoms, examination and test results, our assessment of your condition, a record of your treatment interventions, and a plan for future care or treatment. **We have an ethical and legal obligation to protect the privacy of your health information**, and we will only use or disclose this information in limited circumstances. In general, we may use and disclose your health information to:
> - plan your care and treatment;
> - provide treatment by us or others;
> - communicate with other providers such as referring physicians;
> - receive payment from you, your health plan, or your health insurer;
> - make quality assessments and work to improve the care we render and the outcomes we achieve known as health care operations;
> - make you aware of services and treatments that may be of interest to you; and
> - comply with state and federal laws that require us to disclose your health information. We may also use or disclose your health information where you have authorized us to do so. Although your health record belongs to Progressive Physical Therapy, PC, the information in your record belongs to you.
>
> <u>You have the right to:</u>
> - ensure the accuracy of your health record;
> - request confidential communications between you and your therapist and request limits on the use and disclosure of your health information; and
> - request an accounting of certain uses and disclosures of health information we have made about you.
>
> <u>We are required to:</u>
> - **maintain the privacy of your health information**;
> - provide you with notice, such as this *Notice of Privacy Practices*, as to our legal duties and privacy practices with respect to information we collect and maintain about you;

[8] *Id*.

- abide by the terms of our most current *Notice of Privacy Practices*;
- notify you if we are unable to agree to a requested restriction; and
- accommodate reasonable requests you may have to communicate health information by alternative means or at alternative locations.[9]

28. With regards to a patient's right to receive notice if a breach occurs, the Privacy Notice states the following:

> We are required to notify you by first class mail or by e-mail (if you have indicated a preference to receive information by e-mail), of any breaches of Unsecured Protected Health Information as soon as possible, but in any event, **no later than 60 days following the discovery of the breach**. "Unsecured Protected Health Information" is information that is not secured through the use of a technology or methodology identified by the Secretary of the U.S. Department of Health and Human Services to render the Protected Health Information unusable, unreadable, and undecipherable to unauthorized users.[10]

29. The Privacy Notice states, with respect to business associates, that "[w]e may disclose your health information to our business associates so that they can perform the job we have asked them to do[,]" such as providing transcription, billing, consulting, legal, and answering services.[11]

30. As a condition of purchasing healthcare goods and services from Defendant, SDFC requires that its patients entrust it with highly sensitive personal information.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

32. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

33. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

---

[9] *Id.* (emphasis added).
[10] *Id.* (emphasis added).
[11] *Id.*

THE CYBERATTACK AND DATA BREACH

34. On December 3, 2020,[12] SDFC and its business associate, Health Partners of Southern California ("HCP"), "became aware that [its] information technology hosting provider experienced a data security incident that resulted in the encryption of certain data."[13]

35. After discovering the security incident, an investigation into the incident was launched to determine its nature and scope.[14]

36. On January 21, 2021, the investigation revealed that an unauthorized actor gained access to Defendant's system and that "certain SDFC and HCP data may have been accessed or acquired[,]" which included files containing Plaintiff's and Class Members' Private Information.[15] In addition, the investigation revealed that approximately 125,500 individuals were victims of the Data Breach.[16]

37. SDFC claims it then embarked on a three month review to "identify individuals whose information may have been involved[,]" which ended on April 12, 2021.[17]

38. The "review" revealed that information accessed by the hackers included individuals' names, Social Security numbers or other government identification numbers, financial account numbers, dates of birth, medical diagnoses or treatment information, health insurance information, and/or client identification numbers.[18]

39. SDFC does not assert that the Private Information contained in the files was encrypted.

40. Upon information and belief, the cyberattack targeted Defendant due to its status as a healthcare entity that collects, creates, and maintains both PII and PHI.

---

[12] *See* Submitted Breach Notification Sample – SDFC, State of California Dept. of Justice, *available at:* https://oag.ca.gov/ecrime/databreach/reports/sb24-540686 (last visited June 18, 2021).

[13] *See Notice of Security Incident*, SDFC, *available at:* https://sdfamilycare.org/wp-content/uploads/2021/05/San-Diego-Family-Care-Substitute-Notice.pdf (last visited June 18, 2021).

[14] *Id.*

[15] *Id*.

[16] *Supra*, note 1.

[17] *Supra*, note 14.

[18] *Id.*

41. Upon information and belief, the targeted cyberattack was expressly designed to gain access to private and confidential data, including, among other things, the PII and PHI of employees, former employees, and patients like Plaintiff and Class Members.

42. Because of this targeted cyberattack, data thieves were able to gain access to Defendant's computer network and subsequently access the protected Private Information of Plaintiff and Class Members.

43. While SDFC stated in its "Notice of Data Breach" and "Notice of Security Incident" letters, sent to Plaintiff's and Class Members and posted on its website, respectively, that it learned of the cybersecurity incident in December 2020, SDFC did not begin notifying victims until **May 7, 2021** – approximately **five months** after discovering the Data Breach.

44. In these notices, SDFC openly admits that sensitive patient data stored by SDFC "may have been accessed or acquired by an unauthorized individual."[19] This means that not only did the cybercriminals access and view the Private Information without authorization, but they also removed Plaintiff's and Class Members' Private Information from SDFC's computer network.

45. Plaintiff's and Class Members' Private Information was stolen in the Data Breach. Plaintiff further believe their Private Information was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of all cybercriminals.

46. Defendant had obligations created by HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

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

48. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the

[19] *Id.*

date of the breach.

49. In light of recent high profile data breaches at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

50. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "Entities like smaller municipalities and hospitals are attractive . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[20]

51. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[21]

52. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

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

54. In 2016, the FTC updated its publication, *Protecting Personal Information: A*

---

[20] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), *available at:* https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited June 18, 2021).

[21] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), *available at:* https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited June 18, 2021).

Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[22] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[23]

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

57. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp.*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

58. Defendant failed to properly implement basic data security practices.

---

[22] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 18, 2021).

[23] *Id.*

59. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

60. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

61. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

62. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

63. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protecting physical security systems; protecting against any possible communication system; and training staff regarding critical points.

64. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

65. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

66. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

67. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

68. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. § 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include: 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

69. The Data Breach is considered a breach under the HIPAA Rules because there was an access of PHI not permitted under the HIPAA Privacy Rule. A breach under the HIPAA Rules is defined as, "The acquisition, access, use, or disclosure of [PHI] in a manner not permitted [under the HIPAA Privacy Rule] which compromises the security or privacy of the [PHI]." 45 C.F.R. § 164.402.

70. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate SDFC failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT'S BREACH

71. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. Failing to adequately protect patients' and employees Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing PII and PHI and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

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

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

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

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

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

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

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it has not indicated that it encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

p. Failing to adhere to industry standards for cybersecurity.

72. As the result of computer systems in dire need of security upgrading, inadequate procedures for handling emails containing viruses or other malignant computer code, and an inadequate response to the cyberattack, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access SDFC's computer network and systems which contained unsecured and unencrypted PII.

73. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

74. Cyberattacks and data breaches at healthcare providers like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

75. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[24]

76. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[25]

77. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26] This is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages

---

[24] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), *available at:* https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited June 18, 2021).

[25] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), *available at:* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited June 18, 2021).

[26] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited June 18, 2021).

or phishing emails.

78. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[27]

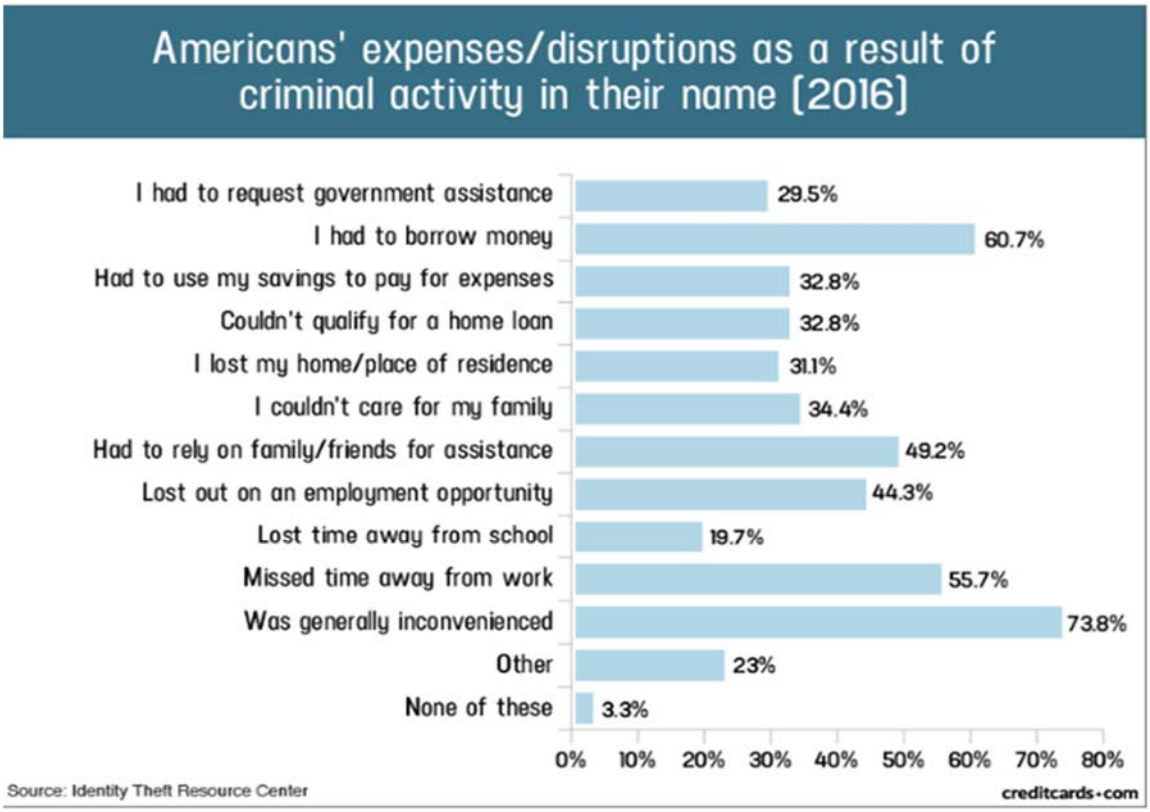
79. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

80. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number or rent a house or receive medical services in the victim's name, and they may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

81. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[28]

[27] *See IdentityTheft.gov*, Federal Trade Commission, *available at:* https://www.identitytheft.gov/Steps (last visited June 18, 2021).

[28] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020), *available at:* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 18, 2021).



82. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.[29]

83. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

84. Theft of PHI, in particular, is gravely serious: A thief may use the victim's name or health insurance numbers to see a doctor, get prescription drugs, file claims with the victim's insurance provider, or get other care. If the thief's health information is mixed with the victim's health information, the victim's treatment, insurance, payment records, and credit report may be

[29] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

affected.[30]

85. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

86. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

87. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at 29.

88. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

89. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

90. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

91. Sensitive Private Information can sell for as much as $363 per record according to

[30] *See* Federal Trade Commission, *Medical Identity Theft*, *available at:* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited June 18, 2021).

the Infosec Institute.[31] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

92. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[32] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[33] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

93. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[34]

94. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x in price on the black market."[35]

---

[31] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at:* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited June 18, 2021).

[32] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1, *available at:* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 18, 2021).

[33] *Id* at 4.

[34] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at:* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited June 18, 2021).

[35] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), *available at:*

95. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[36] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[37]

96. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

97. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet SDFC failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

98. To date, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

99. Defendant has merely offered Plaintiff and Class Members complimentary fraud and identity monitoring services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach. What is more, Defendant places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service as opposed to automatically enrolling all victims of this cybercrime.

100. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

101. Plaintiff was required to provide her Private Information to SDFC in order to receive healthcare services from Defendant.

---

http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 18, 2021).

[36] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), *available at:* https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last visited June 18, 2021).

[37] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), *available at:* https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited June 18, 2021).

102. In or around May 7, 2021, Plaintiff Thomas received notice from SDFC that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Thomas's Private Information, including her name, Social Security Number, date of birth, medical diagnosis or treatment information, health insurance information, client identification information, and other protected health information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

103. As a result of the Data Breach, Plaintiff Thomas made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to: researching the Data Breach; reviewing credit reports, financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by SDFC. Plaintiff Thomas now spends approximately 30 minutes per month reviewing her bank accounts and other sensitive accounts for irregularities. To date, Plaintiff Thomas has spent at least 1 hour on these tasks, valuable time Plaintiff Thomas otherwise would have spent on other activities, including but not limited to work and/or recreation.

104. Plaintiff Thomas is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

105. Plaintiff Thomas suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that SDFC obtained from Plaintiff Thomas; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

106. Moreover, subsequent to the Data Breach, Plaintiff Thomas also experienced a significant increase in the amount of suspicious, unsolicited phishing telephone calls, emails and text messages that she receives. Each day, Plaintiff Thomas receives numerous scam calls, scam emails, and scam texts, all of which appear to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering.

107. As a result of the Data Breach, Plaintiff Thomas anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Thomas will continue to be at increased risk of identity theft and fraud for years to come.

108. Plaintiff's Private Information was compromised as a direct and proximate result of the Data Breach.

109. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

110. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

111. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

112. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

113. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

114. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyberthieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

115. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of SDFC's computer

property and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for and agreed to.

116. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their medical accounts and sensitive information for misuse.

117. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their names;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

118. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

119. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be

disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

120. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

121. Plaintiff brings this action on behalf of themselves and on behalf of all other persons similarly situated.

122. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons SDFC identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").

123. Excluded from the Class are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and Defendant's affiliates, legal representatives, attorneys, successors, heirs, and assigns. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

124. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately 125,500 individuals whose sensitive data was compromised in Data Breach.

125. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA and/or the California Confidentiality of Medical Information Act ("CMIA");

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

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant breached a fiduciary duty to Plaintiff and Class Members;

m. Whether Defendant violated the consumer protection statutes invoked below;

n. Whether Defendant breach implied or express contracts with Plaintiff and Class Members;

o. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

p. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

q. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

126. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

127. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's counsel are competent and experienced in litigating class actions.

128. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

129. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

130. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Class)

131. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 130 above as if fully set forth herein.

132. Defendant required patients, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of rendering healthcare services.

133. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

134. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

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

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

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

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

138. In addition, Cal. Civ. Code § 1798.81.5 requires Defendant to take reasonable steps and employ reasonable methods of safeguarding the PII of Class Members who are California residents.

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

140. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

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

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

141. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

142. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

143. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

144. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Intrusion Upon Seclusion / Invasion of Privacy
(On Behalf of Plaintiff and the Class)

145. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 130 as if fully set forth herein.

146. California established the right to privacy in Article I, Section 1 of the California Constitution.

147. The State of California recognizes the tort of Intrusion into Private Affairs, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

148. Plaintiff and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

149. Defendant's conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion and privacy under common law.

150. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that a person with ordinary sensibilities would consider Defendant's intentional actions or inaction highly offensive and objectionable.

151. In failing to protect Plaintiff's and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

THIRD COUNT
Breach of Express Contract
(On Behalf of Plaintiff and the Class)

152. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 130 as if fully set forth herein.

153. Plaintiff and Class Members allege that they entered into valid and enforceable express contracts, or were third party beneficiaries of valid and enforceable express contracts, with Defendant.

154. The valid and enforceable express contracts that Plaintiff and Class Members entered into with Defendant include Defendant's promise to protect from disclosure nonpublic personal information given to Defendant or that Defendant gathers on its own.

155. Under these express contracts, Defendant and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff and the Class Members' Private Information: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Class Members agreed to pay money for these services, and to turn over their Private Information.

156. Both the provision of healthcare and the protection of Plaintiff's and Class Members' PII/PHI were material aspects of these contracts.

157. At all relevant times, Defendant expressly represented in its Privacy Notice that it would, among other things: keep patients' protected health information (PHI) private; inform patients of its legal duties and comply with laws protecting patients' health information; only use and release patients' health information for approved reasons; provide adequate notice to patients if their Private Information is disclosed without authorization; and adhere to the terms outlined in the Privacy Notice.[38]

158. Defendant's express representations, including, but not limited to, express representations found in its Notice of Privacy Practices, formed an express contract requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII/PHI.

159. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their PII/PHI associated with obtaining healthcare private. To patients such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect PII/PHI is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entered into these contracts with Defendant and/or its affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their PII/PHI would be safeguarded and protected.

160. A meeting of the minds occurred, as Plaintiff and Class Members provided their PII/PHI to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, protection of their PII/PHI.

161. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their PII/PHI.

162. Defendant materially breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was accessed and exfiltrated by unauthorized persons as part of the Data Breach.

163. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not

[38] *Supra*, note 7.

"maintain the privacy" of Plaintiff's and Class Members' PII/PHI as evidenced by its notifications of the Data Breach to Plaintiff and approximately 125,550 Class Members. Specifically, Defendant did not comply with industry standards or otherwise protect Plaintiff's and the Class Members' PII/PHI, as set forth above.

164. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

165. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

166. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

167. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their PII/PHI, the loss of control of their PII/PHI, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

168. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

FOURTH COUNT
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

169. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 130 as if fully set forth herein.

170. When Plaintiff and Class Members provided their Private Information to SDFC in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

171. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

172. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant federal and state laws and regulations and were consistent with industry standards.

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

174. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

175. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

176. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

177. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

178. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

179. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit

to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FIFTH COUNT
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

180. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 130 as if fully set forth herein.

181. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardians of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a data breach and disclosure; and (3) maintain complete and accurate records of what patient information (and where) Defendant did and does store.

182. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of this relationship, in particular, to keep secure the Private Information of its patients.

183. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

184. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

185. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

186. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

187. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

188. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

189. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

190. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

191. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

192. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(4).

193. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, *et seq*.

194. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its

workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

195. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

196. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

197. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

198. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SIXTH COUNT
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

199. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 130 as if fully set forth herein.

200. This count is plead in the alternative to Counts 3 and 4 (breach of express and breach of implied contract).

201. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant money for healthcare services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' PII and PHI, and by providing Defendant with their valuable PII and PHI.

202. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

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

204. Defendant acquired the monetary benefit and PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

205. If Plaintiff and Class Members knew that Defendant had not secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

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

207. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft;

(ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII and PHI in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

209. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from Defendant. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

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

210. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 130 as if fully set forth herein.

211. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization."

212. At all relevant times, Defendant was a health care provider because it had the "purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual." Cal. Civ. Code § 56.06(a).

213. At all relevant times. Defendant collected, stored, managed, and transmitted Plaintiff's and Class Members' PII/PHI.

214. The CMIA requires Defendant to implement and maintain standards of confidentiality with respect to all individually identifiable PHI disclosed to it and maintained by it. Specifically, Cal. Civ. Code § 56.10(a) prohibits Defendant from disclosing Plaintiff's and Class Members' PHI without first obtaining their authorization to do so.

215. Section 56.11 of the California Civil Code specifies the manner in which authorization must be obtained before PHI is released. Defendant, however, failed to obtain any authorization—let alone, proper authorization—from Plaintiff and Class Members before releasing and disclosing their PHI. Defendant also failed to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class Members' PHI as required by California law.

216. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff's and Class Members' PHI was disclosed to unauthorized parties. By disclosing Plaintiff's and Class Members' PHI without their written authorization, Defendant violated Cal. Civ. Code § 56, *et seq*. and its legal duty to protect the confidentiality of such information.

217. Defendant also violated Sections 56.06 and 56.101 of the CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential PHI. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach,

Plaintiff's and Class Members' confidential PHI was viewed by and released and disclosed to unauthorized persons without Plaintiff's and Class Members' authorization.

218. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violation of the CMIA, Plaintiff and Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per plaintiff and Class Member, (iii) injunctive relief, (iv) punitive damages of up to $3,000 per plaintiff and each Class Member, and (v) attorneys' fees, litigation expenses and court costs under Cal. Civ. Code §§ 56.35, 56.36.

EIGHTH COUNT
Violation of the California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff and the Class)

219. Plaintiff repeats and re-alleges each and every allegation contained in Paragraphs 1 through 130 as if fully set forth herein.

220. The California Unfair Competition Law, Cal Bus. & Prof. Code § 17200, *et seq*. prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful and unfair practices within the meaning, and in violation, of the UCL.

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

222. In the course of conducting its business, Defendant committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI, and violating the statutory and common law alleged herein in the process, including, *inter alia*, the CMIA, the FTC Act, and HIPAA. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts

or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

223. Defendant also violated the UCL by failing to timely notify Plaintiff and Class Members regarding the unauthorized release and disclosure of their PII/PHI. If Plaintiff and Class Members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII/PHI, medical information, and identities.

224. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

225. Plaintiff and Class Members relied upon the representations in the Privacy Notice, a copy of which (upon information and belief) was provided to Plaintiff and Class Members prior to the receipt of any medical services from Defendant.

226. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the CMIA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

227. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class Members, and the general public, also seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it, as well as all other relief the Court deems appropriate, consistent with Cal. Bus. & Prof. Code § 17203.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff and her counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

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

DATED: June 18, 2021

Respectfully Submitted,

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP

By: Rachele R. Byrd
RACHELE R. BYRD

BETSY C. MANIFOLD (182450)
RACHELE R. BYRD (190634)
MARISA C. LIVESAY (223247)
BRITTANY N. DEJONG (258766)
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599
manifold@whafh.com
byrd@whafh.com
livesay@whafh.com
dejong@whafh.com

MASON LIETZ & KLINGER LLP
Gary E. Mason (*pro hac vice forthcoming*)
David K. Lietz (*pro hac vice forthcoming*)
5101 Wisconsin Ave., NW, Ste. 305
Washington, DC 20016
Phone: 202.640.1160
dlietz@masonllp.com

Gary M. Klinger (*pro hac vice forthcoming*)
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: (202) 975-0477

gklinger@masonllp.com

M. ANDERSON BERRY
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com

Attorneys for Plaintiff and the Proposed Class

EXHIBIT A

West Sacramento, CA 95798-9728

001794

Dacia Thomas
[redacted]

May 7, 2021

Subject: Notice of Data Breach

Dear Dacia Thomas:

I am writing to inform you of a data security incident that may have affected your personal information. At San Diego Family Care ("SDFC"), we take the privacy and security of your personal information very seriously. We are contacting you to notify you that this incident occurred and inform you about steps you can take to ensure your information is protected, including enrolling in the complimentary identity protection services we are making available to you.

What Happened. In December 2020, SDFC and its business associate, Health Center Partners of Southern California (HCP), became aware that our information technology hosting provider experienced a data security incident that resulted in the encryption of certain data. The hosting provider took steps to secure and restore its systems and launched an investigation with the assistance of computer forensics experts. At that time, SDFC did not know what, if any, data belonging to SDFC or HCP may have been involved in the incident.

On January 20, 2021, we learned that, based on our hosting provider's investigation into the incident, certain SDFC and HCP data may have been accessed or acquired by an unauthorized individual. We obtained a copy of the impacted data and engaged experts to conduct a thorough review to identify individuals whose information may have been involved in the incident. That review concluded on April 12, 2021, and indicated that your information may have been involved.

Please note that this unauthorized access was limited to systems that stored information about insurance claims, and did not affect any other SDFC information systems, such as our electronic medical record system. We are not aware of the misuse of any personal information that may have been affected by this incident.

What Information Was Involved. The affected information may have included your name, Social Security Number, date of birth, medical diagnosis or treatment information, health insurance information, and/or client identification number.

What Are We Doing. As soon as SDFC learned of the incident, we took the steps described above. We are also working with ou hosting provider to ensure that appropriate remediation measures are taken to reduce the likelihood of a similar incident occurring the future. In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expe IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimburseme policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity compromised.

What You Can Do. We recommend that you review the guidance included with this letter about how to protect your informati In addition, you can enroll in the free credit monitoring services that we are offering to you through IDX by calling (833) 664-19 or going to https://response.idx.us/sdfcprotect and using the Enrollment Code provided above.

For More Information. If you have questions or need assistance, please contact (833) 664-1997, Monday through Friday, 6ar 6pm PT. Our representatives are fully versed on this incident and can answer any questions you may have regarding the protect of your personal information.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that may cause you.

Sincerely,

Roberta L. Feinberg

Roberta L. Feinberg, M.S.
Chief Executive Officer
San Diego Family Care