

Exhibit 3

1 Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2 **KEEGAN & BAKER, LLP**
2292 Faraday Avenue, Suite 100
3 Carlsbad, CA 92008
Telephone: (760) 929-9303
4 Facsimile: (760) 929-9260

5 Attorneys for Plaintiff JANE DOE

ELECTRONICALLY FILED
Superior Court of California,
County of San Diego

05/25/2021 at 07:43:48 PM

Clerk of the Superior Court
By Jacqueline J. Walters, Deputy Clerk

6
7 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
8 **FOR THE COUNTY OF SAN DIEGO**

9 JANE DOE, individually and on behalf of all
others similarly situated,

10 Plaintiff,

11 vs.

12 SAN DIEGO FAMILY CARE; and DOE
13 DEFENDANTS 1-100;

14 Defendants.
15
16
17
18

) Case No.: 37-2021-00023006-CU-BT-CTL
)
)

) **CLASS ACTION COMPLAINT FOR**
) **DAMAGES, RESTITUTION, AND**
) **INJUNCTIVE RELIEF FOR VIOLATIONS**
) **OF:**
)

-) (1) **THE CONFIDENTIALITY OF**
) **MEDICAL INFORMATION ACT,**
) **CIVIL CODE §§ 56, ET SEQ.;**
) (2) **BREACH OF CALIFORNIA**
) **SECURITY NOTIFICATION**
) **LAWS, CALIFORNIA CIVIL CODE**
) **§ 1798.82; AND**
) (3) **BUSINESS AND PROFESSIONS**
) **CODE §§ 17200, ET SEQ.**
)

) **JURY TRIAL DEMANDED**
)

19 Plaintiff JANE DOE (or “Plaintiff”), by and through her attorneys, bring this class action on
20 behalf of herself individually and all others similarly situated, against Defendants SAN DIEGO
21 FAMILY CARE and DOE DEFENDANTS 1-100 (collectively referred to as “Defendants”), and
22 alleges upon information and belief as follows:

23 **INTRODUCTION**

24 1. This class action arises from the negligent and failure of Defendants to properly
25 create, maintain, preserve, and/or store confidential, medical and personal identifying information
26 of Plaintiff¹ and all other persons similarly situated which allowed an unauthorized person to gain
27

28 ¹ California statutory law specifically allows a party to bring a lawsuit using a pseudonym in cases
involving health care patients. Cal. Civ. Code § 3427.3 (West 2011). Specifically, section 3427.3

1 access to an email file transfer platform of Defendants prior to and in December of 2020, causing
2 unauthorized access, viewing, exfiltration, theft, and disclosure of unencrypted medical and
3 personal identifying information of Plaintiff and other persons similarly situated, to at least one
4 unauthorized person resulting in violations of the Confidentiality of Medical Information Act, Civil
5 Code §§ 56, *et seq.* (hereinafter referred to as the “Act”), the Security Notification Laws, Civil Code
6 § 1798.82, and the Business and Professions Code §§ 17200 *et seq.* Under the Act, Plaintiff, and
7 all other persons similarly situated, have the right to expect that the confidentiality of their medical
8 information in possession of Defendants and/or derived from Defendants to be reasonably
9 preserved and protected from unauthorized access, viewing, exfiltration, theft, and disclosure.

10 2. As alleged more fully below, failing to take adequate and reasonable measures to
11 ensure its data systems were protected against unauthorized intrusions, by failing to invest in cyber
12 security and data protection safeguards, failing to implement adequate and reasonable security
13 controls and user authorization and authentication processes, failing to limit the types of data
14 permitted to be transferred, failing to properly and adequately educate and train its employees, and
15 to put into place reasonable or adequate computer systems and security practices to safeguard
16 customers’ and patients’ medical and personal identifying information, Defendants negligently
17 created, maintained, preserved, and stored Plaintiff’s and the Class (defined *infra*) members’
18 medical and personal identifying information in possession of or derived from Defendants allowed
19 such information to be accessed, acquired, stolen and viewed by one “unauthorized individual,”
20 without Plaintiff’s and the Class members’ prior written authorization, which constitutes
21 unauthorized disclosure and/or release of their information in violation of Civil Code §§ 56.10(a)
22 and 56.101(a) of the Act. In fact, Defendant SAN DIEGO FAMILY CARE’s form letter, entitled

23
24
25 provides, “The court having jurisdiction over a civil proceeding under this title shall take all steps
26 ***reasonably necessary to safeguard the individual privacy and prevent harassment of a health care***
27 ***patient***, licensed health practitioner, or employee, client, or customer of a health care facility who is
28 a party or witness in the proceeding, including granting protective orders. ***Health care patients***,
licensed health practitioners, and employees, clients, and customers of the health care facility ***may***
use pseudonyms to protect their privacy.” Cal. Civ. Code § 3427.3 (emphasis added). Here, a
pseudonym has been used in place of the real name of Plaintiff because at all times relevant to this
action, Plaintiff is a health care patient under Civil Code § 56.05(k) and has individual privacy
concerns and a reasonable fear of harassment in light of the nature of the case.

1 “Subject: Notice of Data Breach,” dated May 7, 2021, signed by Roberta L. Feinberg, M.S., in her
2 capacity as “Chief Executive Officer” of “San Diego Family Care,” sent to Plaintiff and all other
3 persons similarly situated, stating in part, “I am writing to inform you of a data security incident that
4 may have affected your personal information,” and informing her, in part, of “We are contacting
5 you to notify you that this incident occurred and inform you about steps you can take to ensure your
6 information is protected What Happened. In December 2020, SDFC and its business associate,
7 Health Center Partners of Southern California (HCP), became aware that our information
8 technology hosting provider experienced a data security incident that resulted in the encryption of
9 certain data.... On January 20, 2021, we learned that, based on our hosting provider’s investigation
10 into the incident, certain SDFC and HCP data may have been accessed or acquired by an
11 unauthorized individual. We obtained a copy of the impacted data and engaged experts to conduct a
12 thorough review to identify individuals whose information may have been involved in the
13 incident.... What Information Was Involved. The affected information may have included your
14 name, date of birth, medical diagnosis or treatment information, health insurance information.
15 and/or client identification number.... Please accept our sincere apologies for any worry or
16 inconvenience that this may cause you.” An exemplar of Defendant SAN DIEGO FAMILY
17 CARE’s form letter, entitled “Subject: Notice of Data Breach,” dated May 7, 2021, signed by
18 Roberta L. Feinberg, M.S., in her capacity as “Chief Executive Officer” of “San Diego Family
19 Care,” submitted to the Attorney General of the State of California is attached hereto as **Exhibit A**.

20 3. Because the individually identifiable medical information and other personal
21 identifying information of Plaintiff and the Class was subject to unauthorized access, theft and
22 viewing by at least one “unauthorized individual” and in violation of the Act, Plaintiff, individually
23 and on behalf of all others similarly situated, seeks from Defendants nominal damages in the
24 amount of one thousand dollars (\$1,000) for each violation under Civil Code §56.36(b)(1) and
25 actual damages, according to proof, for each violation pursuant to Civil Code § 56.36(b)(2).
26 Further, because Plaintiff also alleges Defendants’ conduct violates Business & Professions Code
27 §§ 17200, *et seq.*, Plaintiff, individually and on behalf of others similarly situated, seeks injunctive
28 relief and restitution from Defendants under Business and Professions Code § 17203.

1 received a letter at her residential address, sent on SAN DIEGO FAMILY CARE’s behalf,
2 addressed in her name, entitled “Subject: Notice of Data Breach,” dated May 7, 2021, signed by
3 Roberta L. Feinberg, M.S., in her capacity as “Chief Executive Officer” of “San Diego Family
4 Care,” sent to Plaintiff and all other persons similarly situated, stating in part, “I am writing to
5 inform you of a data security incident that may have affected your personal information,” and
6 informing her, in part, of “We are contacting you to notify you that this incident occurred and
7 inform you about steps you can take to ensure your information is protected What Happened. In
8 December 2020, SDFC and its business associate, Health Center Partners of Southern California
9 (HCP), became aware that our information technology hosting provider experienced a data security
10 incident that resulted in the encryption of certain data.... On January 20, 2021, we learned that,
11 based on our hosting provider’s investigation into the incident, certain SDFC and HCP data may
12 have been accessed or acquired by an unauthorized individual. We obtained a copy of the impacted
13 data and engaged experts to conduct a thorough review to identify individuals whose information
14 may have been involved in the incident.... What Information Was Involved. The affected
15 information may have included your name, date of birth, medical diagnosis or treatment
16 information, health insurance information and/or client identification number.... Please accept our
17 sincere apologies for any worry or inconvenience that this may cause you.” An exemplar of
18 Defendant SAN DIEGO FAMILY CARE’s form letter, entitled “Subject: Notice of Data Breach,”
19 dated May 7, 2021, signed by Roberta L. Feinberg, M.S., in her capacity as “Chief Executive
20 Officer” of “San Diego Family Care,” submitted to the Attorney General of the State of California
21 is attached hereto as **Exhibit A**. As a result, Plaintiff reasonably fears that disclosure and/or release
22 of her medical information created, maintained, preserved and/or stored on Defendants’ email and
23 computer network could subject her to harassment or abuse.

24 **B. DEFENDANTS**

25 9. Defendant SAN DIEGO FAMILY CARE (“SDFC”) is registered to do business and
26 does business in the State of California (Entity File No. C0635826), operates a principal place of
27 business located at 6973 Linda Vista Road, San Diego, CA 92111. At all times relevant to this
28 action, SDFC was and is a provider of health care who created, maintained, preserved, and stored

1 personal and confidential medical information, as that term is defined and set forth in the Act,
2 including the names, dates of birth, medical diagnosis or treatment information, health insurance
3 information and/or client identification numbers, of Plaintiff and the Class (defined *infra*), and is
4 subject to the requirements and mandates of the Act, including but not limited to Civil Code §§
5 56.10, 56.101 and 56.36. On its website, SDFC represents that “San Diego Family Care operates
6 eight (8) health centers in San Diego County. This includes 4 sites in Linda Vista, the Mid-City
7 Community Clinic (Adults) and the Mid-City Community Clinic (Pediatrics), as well as two (2)
8 school based clinics inside elementary and middle schools. These high quality community health
9 centers deliver 116,337 primary care medical, dental and mental health visits annually to all
10 residents of San Diego County.”² On its website, SDFC represents that “Welcome to San Diego
11 Family Care. HealthCare Support Portal facilitates better communication with your physician’s
12 office by providing convenient 24 x 7 access from the comfort and privacy of your own home or
13 office.”³ On or about May 7, 2021, SDFC caused a form letter sent on its behalf, entitled “Subject:
14 Notice of Data Breach,” dated May 7, 2021, signed by Roberta L. Feinberg, M.S., in her capacity
15 as “Chief Executive Officer” of “San Diego Family Care,” an exemplar of which is attached hereto
16 as **Exhibit A**, to be submitted to the Attorney General of the State of California and to be mailed to
17 Plaintiff and all others similarly situated. Thus, at all times relevant to this action, SDFC was and is
18 a provider of health care and employed and employs persons located in the County of San Diego
19 and in this judicial district.

20 10. At all times relevant to this action, SDFC was and is a “business” within the meaning
21 of Civil Code § 1798.140(c)(1), owns or licenses computerized data which includes Plaintiff’s and
22 the Class’ personal information, within the meaning of Civil Code § 1798.82(h), collected
23 Plaintiff’s and the Class’ personal information within the meaning of Civil Code §
24 1798.81.5(d)(1)(A).

25
26
27

28 ² (<https://sdfamilycare.org/about-sdfc/>, last visited May 25, 2021).

³ (https://mycw17.eclinicalweb.com/portal948/jsp/100mp/login_otp.jsp, last visited May 25, 2021).

1 **C. DOE DEFENDANTS**

2 11. The true names and capacities, whether individual, corporate, associate, or otherwise,
3 of Defendants sued herein as DOE DEFENDANTS 1 through 100, inclusive, are currently unknown
4 to Plaintiff, who therefore sues the Defendants by such fictitious names under the Code of Civil
5 Procedure § 474. Each of the Defendants designated herein as a DOE DEFENDANT is legally
6 responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of
7 court and/or amend this complaint to reflect the true names and capacities of the Defendants
8 designated hereinafter as DOE DEFENDANTS 1 through 100 when such identities become known.
9 Any reference made to a named Defendant by specific name or otherwise, individually or plural, is
10 also a reference to the actions or inactions of DOE DEFENDANTS 1 through 100, inclusive.

11 **D. AGENCY/AIDING AND ABETTING**

12 12. At all times herein mentioned, Defendants, and each of them, were an agent or joint
13 venturer of each of the other Defendants, and in doing the acts alleged herein, were acting with the
14 course and scope of such agency. Each Defendant had actual and/or constructive knowledge of the
15 acts of each of the other Defendants, and ratified, approved, joined in, acquiesced and/or authorized
16 the wrongful acts of each co-defendant, and/or retained the benefits of said wrongful acts.

17 13. Defendants, and each of them, aided and abetted, encouraged and rendered
18 substantial assistance to the other Defendants in breaching their obligations to Plaintiff and the
19 Class, as alleged herein. In taking action, as particularized herein, to aid and abet and substantially
20 assist the commissions of these wrongful acts and other wrongdoings complained of, each of the
21 Defendants acted with an awareness of his/her/its primary wrongdoing and realized that his/her/its
22 conduct would substantially assist the accomplishment of the wrongful conduct, wrongful goals,
23 and wrongdoing.

24 **FACTUAL ALLEGATIONS**

25 14. At all times relevant to this action, including the period prior to and in December
26 2020, SDFC created, maintained, preserved, and stored records of the care, services and products,
27 including the names, dates of birth, medical diagnosis or treatment information, health insurance
28 information and/or client identification numbers of Plaintiff and the Class (all of which constitutes

1 medical information, as that term is defined and set forth in the Act), that Plaintiff and other Class
2 members received in the State of California from SDFC and other SDFC providers of health care,
3 on its email and computer network. As a result, at all times relevant to this action, including the
4 period prior to and in December 2020, SDFC was and is a “provider of health care” within the
5 meaning of Civil Code § 56.05(m). As a result, at all times relevant to this action, including the
6 period prior to and in December 2020, Plaintiff and Class members were patients, within the
7 meaning of Civil Code § 56.05(k), of SDFC and/or other SDFC providers of health care.

8 15. As a result, prior to and in December 2020, Defendants possessed Plaintiff’s and the
9 Class’ medical information, in electronic and physical form, in possession of or derived
10 from Defendants regarding their medical history, mental or physical condition, or treatment. Such
11 medical information included or contained an element of personal identifying information sufficient
12 to allow identification of Plaintiff and the Class, such as their names, addresses, dates of birth,
13 social security numbers, phone numbers and/or email addresses, or other information that, alone or
14 in combination with other publicly available information, reveals their identity.

15 16. At all times relevant to this action, including the period prior to and in December
16 2020, pursuant to Civil Code § 56.06(a), SDFC, as a business that created, maintained, preserved,
17 and stored records of the care, products and services that the Class members received in the State of
18 California from SDFC and/or other SDFC providers of health care, and/or other health care service
19 plans, pharmaceutical companies, and contractors as defined by the Act, is and was, at all times
20 relevant to this action, organized for the purpose of maintaining medical information, within the
21 meaning of Civil Code § 56.05(j), in order to make the information available to an individual or to a
22 provider of health care at the request of the individual or a provider of health care, for purposes of
23 allowing the individual to manage his or her information, or for the diagnosis and treatment of the
24 individual, is deemed to be a “provider of health care,” within the meaning of Civil Code §
25 56.05(m).

26 17. Alternatively, at all times relevant to this action, including prior to and in December
27 2020, pursuant to Civil Code § 56.05(d), SDFC, as an entity that is a medical group, independent
28 practice association, pharmaceutical benefits manager, or a medical service organization and is not a

1 health care service plan or provider of health care, is and was a “contractor” under Civil Code §
2 56.05(d).

3 18. Alternatively, at all times relevant to this action, including prior to and in December
4 2020, pursuant to Civil Code § 56.13, SDFC is and was a recipient of medical information pursuant
5 to an authorization as provided by the Act or pursuant to the provisions of subdivision (c) of Section
6 56.10 and was prohibited from further disclosing that medical information except in accordance
7 with a new authorization that meets the requirements of Section 56.11, or as specifically required or
8 permitted by other provisions of the Act or by law.

9 19. Alternatively, at all times relevant to this action, including prior to and in December
10 2020, pursuant to Civil Code § 56.245, SDFC is and was a recipient of medical information
11 pursuant to an authorization as provided by this chapter, and was prohibited from further disclosing
12 such medical information unless in accordance with a new authorization that meets the requirements
13 of Section 56.21, or as specifically required or permitted by other provisions of the Act or by law.

14 20. Additionally, at all times relevant to this action, including prior to and in December
15 2020, pursuant to Civil Code § 56.26(a), SDFC is and was an entity engaged in the business of
16 furnishing administrative services to programs that provide payment for health care services, and
17 was prohibited from knowingly using, disclosing or permitting its employees or agents to use or
18 disclose medical information possessed in connection with performing administrative functions for
19 a program, except as reasonably necessary in connection with the administration or maintenance of
20 the program, or as required by law, or with an authorization.

21 21. As a provider of health care, a contractor, and/or other authorized recipient of
22 personal and confidential medical information, SDFC is required by the Act to ensure that medical
23 information regarding patients is not disclosed or disseminated or released without patients’
24 authorization, and to protect and preserve the confidentiality of the medical information regarding a
25 patient, under Civil Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36.

26 22. As provider of health care, a contractor, and/or other authorized recipient of personal
27 and confidential medical information, SDFC is required by the Act not to disclose medical
28

1 information regarding a patient without first obtaining an authorization⁴ under Civil Code §§ 56.10,
2 56.13, 56.245 and 56.26.

3 23. As a provider of health care, a contractor, and/or other authorized recipient of
4 personal and confidential medical information, SDFC is required by the Act to create, maintain,
5 preserve, and store medical records in a manner that preserves the confidentiality of the information
6 contained therein under Civil Code § 56.101(a).

7 24. As provider of health care, a contractor, and/or other authorized recipient of personal
8 and confidential medical information, SDFC is required by the Act to protect and preserve
9 confidentiality of electronic medical information of Plaintiff and the Class in its possession under
10 Civil Code § 56.101(b)(1)(A).

11 25. As a provider of health care, a contractor, and/or other recipient of medical
12 information, SDFC is required by the Act to take appropriate preventive actions to protect the
13 confidential information or records against release consistent with SDFC's obligations under the
14

15 ⁴ An "authorization" is defined under the Act as obtaining permission in accordance with Civil Code § 56.11. Under
16 Civil Code § 56.11, an authorization for the release of medical information is valid only if it:

17 (a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.

18 (b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no
19 other purpose than to execute the authorization.

20 (c) Is signed and dated by one of the following:

21 (1) The patient. A patient who is a minor may only sign an authorization for the release of medical information obtained
22 by a provider of health care, health care service plan, pharmaceutical company, or contractor in the course of furnishing
23 services to which the minor could lawfully have consented under Part 1 (commencing with Section 25) or Part 2.7
24 (commencing with Section 60).

25 (2) The legal representative of the patient, if the patient is a minor or an incompetent. However, authorization may not
26 be given under this subdivision for the disclosure of medical information obtained by the provider of health care, health
27 care service plan, pharmaceutical company, or contractor in the course of furnishing services to which a minor patient
28 could lawfully have consented under Part 1 (commencing with Section 25) or Part 2.7 (commencing with Section 60).

(3) The spouse of the patient or the person financially responsible for the patient, where the medical information is
being sought for the sole purpose of processing an application for health insurance or for enrollment in a nonprofit
hospital plan, a health care service plan, or an employee benefit plan, and where the patient is to be an enrolled spouse
or dependent under the policy or plan.

(4) The beneficiary or personal representative of a deceased patient.

(d) States the specific uses and limitations on the types of medical information to be disclosed.

(e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or
contractor that may disclose the medical information.

(f) States the name or functions of the persons or entities authorized to receive the medical information.

(g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to
receive the medical information.

(h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or
contractor is no longer authorized to disclose the medical information.

(i) Advises the person signing the authorization of the right to receive a copy of the authorization.

1 Act, under Civil Code § 56.36(e)(2)(E), or other applicable state law, and the Health Insurance
2 Portability and Accountability Act of 1996 (Public Law 104-191) (HIPAA) and all HIPAA
3 Administrative Simplification Regulations in effect on January 1, 2012, contained in Parts 160, 162,
4 and 164 of Title 45 of the Code of Federal Regulations, and Part 2 of Title 42 of the Code of
5 Federal Regulations, including, but not limited to, all of the following:

- 6 i. Developing and implementing security policies and procedures.
- 7 ii. Designating a security official who is responsible for developing and implementing
8 its security policies and procedures, including educating and training the workforce.
- 9 iii. Encrypting the information or records, and protecting against the release or use of
10 the encryption key and passwords, or transmitting the information or records in a
11 manner designed to provide equal or greater protections against improper
12 disclosures.

13 26. At all times relevant to this action, including the period prior to and in December
14 2020, SDFC created, maintained, preserved, and stored Plaintiff's and the Class members' medical
15 information using its information technology hosting provider in an un-encrypted format.

16 27. At all times relevant to this action, including the period prior to and in December
17 2020, SDFC created, maintained, preserved, stored, disclosed and/or delivered Plaintiff's and the
18 Class members' medical information using its information technology hosting provider. At all
19 times relevant to this action, SDFC did not obtain written authorization from the Plaintiff and the
20 Class prior to creating, maintaining, preserving, storing, disclosing and/or delivering Plaintiff's and
21 the Class members' medical information using its information technology hosting provider.
22 Furthermore, SDFC's disclosure of and/or delivery of Plaintiff's and the Class members' medical
23 information using its information technology hosting provider was not permissible without written
24 authorization from the Plaintiff and the Class or under any exemption under Civil Code § 56.10(c).

25 28. By law, the HIPAA Privacy Rule applies only to covered entities, e.g. health care
26 providers. However, most health care providers do not carry out all of their health care activities
27 and functions by themselves. Instead, they often use the services of a variety of other persons or
28 businesses. The Privacy Rule allows covered providers to disclose protected health information

1 (PHI) to these “business associates” if the providers obtain assurances that the business associate
2 will use the information only for the purposes for which it was engaged by the covered entity, will
3 safeguard the information from misuse, and will help the covered entity comply with some of the
4 covered entity’s duties under the Privacy Rule. Covered entities may disclose PHI to an entity in its
5 role as a business associate only to help the covered entity carry out its health care functions – not
6 for the business associate’s independent use or purposes, except as needed for the proper
7 management and administration of the business associate. The Privacy Rule requires that a covered
8 entity obtain assurances from its business associate that the business associate will appropriately
9 safeguard the PHI it receives or creates on behalf of the covered entity. The satisfactory assurances
10 must be in writing, whether in the form of a contract or other agreement between the covered entity
11 and the business associate.

12 29. When hiring and monitoring a service provider or business associate, SDFC knew or
13 should have known that it had a duty to inquire about potential service providers’ and business
14 associates’ cybersecurity programs and how such programs are maintained. SDFC knew or should
15 have known that it had a duty to compare potential service providers’ and business associates’
16 cybersecurity programs to the industry standards adopted by other healthcare providers, and should
17 evaluate potential service providers’ track records in the industry by reviewing public information
18 about data security incidents and litigation. SDFC knew or should have known that it had a duty to
19 also ask potential service providers and business associates about whether they have experienced
20 any cybersecurity incidents and how such incidents were handled, as well as whether the potential
21 service provider has an insurance policy in place that would cover losses caused by cybersecurity
22 breaches (including losses caused by internal and external threats). SDFC knew or should have
23 known that it had a duty to review service provider and business associates contracts to ensure that
24 the contracts require the service providers to comply, on an ongoing basis, with cybersecurity and
25 information security standards (and avoid contract provisions that limit service providers’
26 responsibility for cybersecurity and information technology breaches). Finally, SDFC knew or
27 should have known that it had a duty to pay particular attention to contract terms relating to
28

1 confidentiality, the use and sharing of information, notice by the vendor of cybersecurity risk
2 assessments and audit reports, cybersecurity breaches and records retention and destruction.

3 30. Alternatively, Plaintiff alleges on information and belief that SDFC's disclosure of
4 and/or delivery of Plaintiff's and the Class members' medical information using its information
5 technology hosting provider (presently unknown to Plaintiff) was either without a business
6 associate agreement or pursuant to a business associate agreement that was not permissible under
7 the Privacy Rule or any exemption under Civil Code § 56.10(c), and/or because SDFC negligently
8 failed to obtain reasonable assurances and negligently failed to monitor and conduct assessments of
9 its information technology hosting provider to verify that its information technology hosting
10 provider would comply with HIPAA privacy regulations and to follow guidelines and policies to
11 maintain the privacy, confidentiality, including by encryption, and otherwise reasonably protect
12 Plaintiff's and the Class' medical information from disclosure and/or release to at least one
13 "unauthorized individual" prior to and after SDFC's creating, maintaining, preserving, storing,
14 disclosing and/or delivering Plaintiff's and the Class members' medical information on its
15 information technology hosting provider's "systems that stored information."

16 31. At all times relevant to this action, including the period prior to and in December
17 2020, at least one "unauthorized individual" "accessed" and "acquired" "certain files SDFC [] data"
18 present on its information technology hosting provider's "systems that stored information"
19 containing Plaintiff's and the Class' medical information, including names, dates of birth, medical
20 diagnosis or treatment information, health insurance information and/or client identification
21 numbers, as determined by SDFC's investigation, in an un-encrypted format, as represented by
22 SDFC in its form letter, entitled "Subject: Notice of Data Breach," dated May 7, 2021, signed by
23 Roberta L. Feinberg, M.S., in her capacity as "Chief Executive Officer" of "San Diego Family
24 Care," attached hereto as **Exhibit A**. Thus, at least one "unauthorized individual" "accessed,"
25 "acquired" and actually viewed Plaintiff's and the Class' un-encrypted medical information,
26 including their names, dates of birth, medical diagnosis or treatment information, health insurance
27 information and/or client identification numbers, that, alone or in combination with other publicly
28 available information, reveals their identity.

1 32. SDFC had the resources necessary to protect and preserve confidentiality of
2 electronic medical information of Plaintiff and the Class in their possession, but neglected to
3 adequately implement data security measures as required by HIPPA and the Act, despite their
4 obligation to do so.

5 33. Additionally, the risk of vulnerabilities in its computer and data systems of being
6 exploited by an unauthorized third party trying to steal Plaintiff’s and the Class’ electronic
7 personally identifying and medical information was foreseeable and/or known to SDFC. The
8 California Data Breach Report 2012-2015, issued in February 2016 by Attorney General, Kamala
9 D. Harris, reported, “Malware and hacking presents the greatest threat, both in the number of
10 breaches and the number of records breached” and “Social Security numbers and medical
11 information – was breached than other data types.” Moreover, as Attorney General further reported,
12 just because “[e]xternal adversaries cause most data breaches, [] this does not mean that
13 organizations are solely victims; they are also stewards of the data they collect and maintain. People
14 entrust businesses and other organizations with their data on the understanding that the
15 organizations have a both an ethical and a legal obligation to protect it from unauthorized access.
16 Neglecting to secure systems and data opens a gateway for attackers, who take advantage of
17 uncontrolled vulnerabilities.” Regarding encryption, Attorney General instructed in California Data
18 Breach Report 2012-2015, “As we have said in the past, breaches of this type are preventable.
19 Affordable solutions are widely available: strong full-disk encryption on portable devices and
20 desktop computers when not in use.[] Even small businesses that lack full time information security
21 and IT staff can do this. They owe it to their patients, customers, and employees to do it now.”

22 34. More recently the HIPAA Journal posted on November 1, 2018 warned, “Healthcare
23 organization[s] need to ensure that their systems are well protected against cyberattacks, which
24 means investing in technologies to secure the network perimeter, detect intrusions, and block
25 malware and phishing threats.”

26 35. Further, it also was foreseeable and/or known to SDFC that negligently creating,
27 maintaining, preserving, and/or storing Plaintiff’s and the Class’ medical and personal identifying
28 information, in electronic form, in its email and computer network, including on SDFC’s

1 information technology hosting provider’s “systems that stored information,” in a manner that did
2 not preserve the confidentiality of the information could have a devastating effect on them. As
3 reported in the California Data Breach Report 2012-2015, “There are real costs to individuals.
4 Victims of a data breach are more likely to experience fraud than the general public, according to
5 Javelin Strategy & Research. In 2014, 67 percent of breach victims in the U.S. were also victims of
6 fraud, compared to just 25 percent of all consumers.”

7 36. To be successful, phishing relies on a series of affirmative acts by a company and its
8 employees such as clicking a link, downloading a file, or providing sensitive information. Once
9 criminals gained access to the email accounts of a company and its employees, the email servers
10 communicated—that is, disclosed—the contents of those accounts to the criminals. “Phishing
11 scams are one of the most common ways hackers gain access to sensitive or confidential
12 information. Phishing involves sending fraudulent emails that appear to be from a reputable
13 company, with the goal of deceiving recipients into either clicking on a malicious link or
14 downloading an infected attachment, usually to steal financial or confidential information.”
15 (<https://www.varonis.com/blog/data-breach-statistics/>). As posted on April 21, 2020, the FBI had
16 issued a fresh warning [Alert Number MI-000122-MW] following an increase in COVID-19
17 phishing scams targeting healthcare providers.

18 37. At all times relevant to this action, including the period prior to and in December
19 2020, Defendants negligently created, maintained, preserved, and/or stored Plaintiff’s and the Class’
20 medical information, including Plaintiff’s and the Class’ names, dates of birth, medical diagnosis or
21 treatment information, health insurance information and/or client identification numbers, in
22 electronic form, onto Defendants’ email and computer network, including on SDFC’s information
23 technology hosting provider’s “systems that stored information,” in a manner that did not preserve
24 the confidentiality of the information, and negligently failed to protect and preserve confidentiality
25 of electronic medical information of Plaintiff and the Class in their possession against unauthorized
26 disclosure and/or release, including but not limited to, by failing to conduct and require adequate
27 employee education and training, failing to adequately review & revise information security, failing
28 to have adequate information security, and failing to have adequate privacy policies and procedures

1 in place, as required by the Act, under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a),
2 56.101(b)(1)(A), and 56.36(e)(2)(E), and according to their written representations to Plaintiff and
3 the Class.

4 38. Had SDFC and/or its employees (presently unknown to Plaintiff) taken such
5 appropriate preventive actions, fix the deficiencies in their email accounts, email and computer
6 network, and data security systems, and adopted security measures as required by HIPPA and the
7 Act prior to and in December 2020, SDFC could have prevented Plaintiff's and the Class' electronic
8 medical information from being accessed, acquired, stolen and viewed by at least one "unauthorized
9 individual."

10 39. Prior to and in December 2020, SDFC and/or its employees (presently unknown to
11 Plaintiff), by negligently creating, maintaining, preserving, and storing the electronic medical
12 information of Plaintiff and the Class in their email and computer network, including on SDFC's
13 information technology hosting provider's "systems that stored information," allowed Plaintiff's
14 and the Class' individually identifiable medical information to be accessed, acquired, stolen and
15 viewed by at least one "unauthorized individual," without first obtaining an authorization,
16 constituting a disclosure in violation of Civil Code §§ 56.10(a), 56.13, 56.245 and 56.26(a).

17 40. Prior to and in December 2020, SDFC and/or its employees (presently unknown to
18 Plaintiff), by negligently creating, maintaining, preserving, and storing the electronic medical
19 information of Plaintiff and the Class in their email and computer network, including on SDFC's
20 information technology hosting provider's "systems that stored information," allowed Plaintiff's
21 and the Class' individually identifiable medical information to be accessed, acquired, stolen and
22 viewed by at least one "unauthorized individual," constituting a release in violation of Civil Code §
23 56.101(a).

24 41. Prior to and in December 2020, SDFC and/or its employees (presently unknown to
25 Plaintiff), by negligently creating, maintaining, preserving, and storing the electronic medical
26 information of Plaintiff and the Class in their email and computer network, including on SDFC's
27 information technology hosting provider's "systems that stored information," allowed Plaintiff's
28 and the Class' individually identifiable medical information to be accessed, acquired, stolen and

1 viewed by at least one “unauthorized individual,” constituting a release in violation of Civil Code §
2 56.101(a).

3 42. Prior to and in December 2020, SDFC’s and/or its employees’ negligent failure to
4 protect and preserve confidentiality of electronic medical information of Plaintiff and the Class in
5 their email and computer network, including on SDFC’s information technology hosting provider’s
6 “systems that stored information,” allowed Plaintiff’s and the Class’ individually identifiable
7 medical information to be accessed, acquired, stolen and viewed by at least one “unauthorized
8 individual,” constituting a release in violation of Civil Code § 56.101(b)(1)(A).

9 43. California law requires a business to notify any California resident whose
10 unencrypted personal information, as defined, was acquired, or reasonably believed to have been
11 acquired, by an unauthorized person. California law also requires that a sample copy of a breach
12 notice sent to more than 500 California residents must be provided to the California Attorney
13 General. On or about April 6, 2021, SDFC caused a form letter sent on its behalf, entitled “Subject:
14 Notice of Data Breach,” dated May 7, 2021, signed by Roberta L. Feinberg, M.S., in her capacity
15 as “Chief Executive Officer” of “San Diego Family Care,” an exemplar of which is attached hereto
16 as **Exhibit A**, to be submitted to the Attorney General of the State of California and to be mailed to
17 Plaintiff and the Class, stating in part, “I am writing to inform you of a data security incident that
18 may have affected your personal information,” and informing her, in part, of “We are contacting
19 you to notify you that this incident occurred and inform you about steps you can take to ensure your
20 information is protected What Happened. In December 2020, SDFC and its business associate,
21 Health Center Partners of Southern California (HCP), became aware that our information
22 technology hosting provider experienced a data security incident that resulted in the encryption of
23 certain data.... On January 20, 2021, we learned that, based on our hosting provider’s investigation
24 into the incident, certain SDFC and HCP data may have been accessed or acquired by an
25 unauthorized individual. We obtained a copy of the impacted data and engaged experts to conduct a
26 thorough review to identify individuals whose information may have been involved in the
27 incident.... What Information Was Involved. The affected information may have included your
28 name, date of birth, medical diagnosis or treatment information, health insurance information.

1 and/or client identification number.... Please accept our sincere apologies for any worry or
2 inconvenience that this may cause you.” Further, because SDFC submitted its form letter to the
3 Attorney General of the State of California and mailed it to Plaintiff and the Class, SDFC concedes
4 that Plaintiff’s and the Class’ identifiable medical information contained in email and computer
5 network, including on SDFC’s information technology hosting provider’s “systems that stored
6 information,” was unencrypted and thus, the unauthorized third party or parties who “accessed” and
7 “acquired” Plaintiff’s and the Class’ identifiable medical information was able to and did actually
8 view Plaintiff’s and the Class’ electronic medical information contained in and “acquired” from
9 SDFC’s email and computer network, including on SDFC’s information technology hosting
10 provider’s “systems that stored information.” Thus, at least one “unauthorized individual”
11 “accessed,” “acquired” and actually viewed Plaintiff’s and the Class’ un-encrypted medical
12 information, including their names, dates of birth, medical diagnosis or treatment information,
13 health insurance information and/or client identification numbers, that, alone or in combination with
14 other publicly available information, reveals their identity.

15 44. SDFC’s form letter submitted to the Attorney General of the State of California and
16 mailed to Plaintiff and the Class, attached hereto as **Exhibit A**, concludes by making the following
17 hollow gesture, “Please accept our sincere apologies for any worry or inconvenience that this may
18 cause you.” Other than offering its “apolog[y]” and 12 months of “complimentary identity
19 protection services,” SDFC’s form letter does nothing to further protect Plaintiff and the Class from
20 future incidents of identity theft despite the severity of the unauthorized access, viewing,
21 exfiltration, theft, disclosure and release of their electronic medical and personal information caused
22 by SDFC’s violations of its duty to implement and maintain reasonable security procedures and
23 practices. To date, other than offering its “apolog[y]” and “identity monitoring at no cost to you for
24 one year,” SDFC has not offered any monetary compensation for the unauthorized disclosure and/or
25 release of Plaintiff’s and the Class’ electronic medical information under the Act. In effect, SDFC
26 is shirking its responsibility for the harm it has caused, while shifting the burdens and costs of its
27 wrongful conduct onto its patients, i.e. Plaintiff and the Class.

28

1 CLASS ACTION ALLEGATIONS

2 45. Plaintiff brings this action on behalf of herself individually and on behalf of all
3 others similarly situated. The putative class that Plaintiff seeks to represent is defined as follows:

4 Class: All persons to whom San Diego Family Care sent a letter entitled “Notice
5 of Data Breach” regarding a data security incident that occurred in December
6 2020, an exemplar of which is attached hereto as **Exhibit A**.

7 The officers, directors, and employees of SDFC are excluded from the Class. Plaintiff reserves the
8 right under California Rule of Court 3.765 to amend or modify the Class definition with greater
9 particularity or further division into subclasses or limitation to particular issues as warranted, and as
10 additional facts are discovery by Plaintiff during her future investigations.

11 46. This action is properly maintainable as a class action. The members of the Class are
12 so numerous that joinder of all members is impracticable, if not completely impossible. While the
13 exact number of the Class members is unknown to Plaintiff at this time, SDFC filed a report with
14 the California Attorney General, on or about May 7, 2021, indicating that this security incident
15 affected at least 500 persons. The disposition of the claims of the members of Class through this
16 class action will benefit both the parties and this Court. In addition, the Class is readily identifiable
17 from information and records in the possession of SDFC and its agents, and the Class is defined in
18 objective terms that make the eventual identification of Class members possible and/or sufficient to
19 allow members of the Class to identify themselves as having a right to recover.

20 47. There is a well-defined community of interest among the members of the Class
21 because common questions of law and fact predominate, Plaintiff’s claims are typical of the
22 members of the Class, and Plaintiff can fairly and adequately represent the interests of the Class.

23 48. Common questions of law and fact exist as to all members of the Class and the Class
24 and predominate over any questions affecting solely individual members of the Class and the Class.
25 Among the questions of law and fact common to the Class that predominate over questions which
26 may affect individual Class members, including the following:

- 27 a) Whether Defendants possessed Plaintiff’s and the Class’ medical and personal
28 identifying information prior to and in December 2020;

- 1 b) Whether Defendants created, maintained, preserved and/or stored Plaintiff's and the
2 Class' medical and personal identifying information, in electronic form, onto
3 Defendants' email and computer network prior to and in December 2020;
- 4 c) Whether Defendants implemented and maintained reasonable security procedures
5 and practices to protect Plaintiff's and the Class' medical and personal identifying
6 information, in electronic form, within Defendants' email and computer network
7 prior to and in December 2020;
- 8 d) Whether Plaintiff's and the Class' medical and personal identifying information, in
9 electronic form, within Defendants' email and computer network prior to and in
10 December 2020 was accessed, viewed, exfiltrated and/or publicly exposed by an
11 unauthorized third party;
- 12 e) Whether Plaintiff's and the Class' medical and personal identifying information, in
13 electronic form, within Defendants' email and computer network prior to and in
14 December 2020 was accessed, viewed, exfiltrated and/or publicly exposed by an
15 unauthorized third party without the prior written authorization of Plaintiff and the
16 Class, as required by Civil Code §§ 56.10 and 56.26;
- 17 f) Whether Defendants' creation, maintenance, preservation and/or storage of
18 Plaintiff's and the Class' medical and personal identifying information, in electronic
19 form, within Defendants' email and computer networks, accessed, viewed,
20 exfiltrated and/or publicly exposed by an unauthorized third party was permissible
21 without written authorization from Plaintiff and the Class or under any exemption
22 under Civil Code § 56.10(c);
- 23 g) Whether Defendants' creation, maintenance, preservation and/or storage of
24 Plaintiff's and the Class' medical and personal identifying information, in electronic
25 form, within Defendants' email and computer network, accessed, viewed, exfiltrated
26 and/or publicly exposed by an unauthorized third party constitutes a release in
27 violation of Civil Code §56.101;
- 28

- 1 h) Whether the timing of Defendants' notice that Plaintiff's and the Class' medical and
- 2 personal identifying information, in electronic form, was accessed, viewed,
- 3 exfiltrated and/or publicly exposed by an unauthorized third party, was given in the
- 4 most expedient time possible and without reasonable delay;
- 5 i) Whether Defendants' conduct constitute unlawful, fraudulent or unfair practices in
- 6 violation of Business and Professions Code §§ 17200, *et seq.*; and
- 7 j) Whether Plaintiff and the Class are entitled to actual, nominal or statutory damages,
- 8 injunctive relief and/or restitution.

9 49. Plaintiff's claims are typical of those of the other Class members because Plaintiff,

10 like every other Class member, was exposed to virtually identical conduct and now suffer from the

11 same violations of the law as other Class members.

12 50. Plaintiff will fairly and adequately protect the interests of the Class. Moreover,

13 Plaintiff has no interest that is contrary to or in conflict with those of the Class she seeks to

14 represent. In addition, Plaintiff has retained competent counsel experienced in class action litigation

15 to further ensure such protection and intend to prosecute this action vigorously.

16 51. The nature of this action and the nature of laws available to Plaintiff and the

17 members of Class make the use of the class action format a particularly efficient and appropriate

18 procedure to afford relief to Plaintiff and Class for the claims alleged and the disposition of whose

19 claims in a class action will provide substantial benefits to both the parties and the Court because:

- 20 a) If each member of the Class were required to file an individual lawsuit, SDFC
- 21 would necessarily gain an unconscionable advantage since they would be able to
- 22 exploit and overwhelm the limited resources of each individual member of the Class
- 23 with its vastly superior financial and legal resources;
- 24 b) The costs of individual suits could unreasonably consume the amounts that would be
- 25 recovered;
- 26 c) Proof of a common business practice or factual pattern which Plaintiff experienced is
- 27 representative of that experienced by the Class and will establish the right of each of
- 28 the members to recover on the causes of action alleged;

- 1 d) Individual actions would create a risk of inconsistent results and would be
- 2 unnecessary and duplicative of this litigation;
- 3 e) SDFC has acted or refused to act on grounds generally applicable to the Class as a
- 4 whole, thereby making it appropriate to render judgment with respect to the Class as
- 5 a whole in this litigation; and
- 6 f) The disposition of the claims of the members of Class through this class action will
- 7 produce salutary by-products, including a therapeutic effect upon those who indulge
- 8 in unlawful practices, and aid to legitimate business enterprises by curtailing
- 9 unlawful competition.

10 52. The prosecution of separate actions by individual members of the Class would create
11 a risk of inconsistent or varying adjudications with respect to individual members of the Class,
12 which would establish incompatible standards of conduct for the Defendants in the State of
13 California and would lead to repetitious trials of the numerous common questions of fact and law in
14 the State of California. Plaintiff knows of no difficulty that will be encountered in the management
15 of this litigation that would preclude its maintenance as a class action. As a result, a class action is
16 superior to other available methods for the fair and efficient adjudication of this controversy.

17 53. Notice to the members of the Class may be made by e-mail or first-class mail
18 addressed to all persons who have been individually identified by Defendants and who have been
19 given notice of the data breach.

20 54. Plaintiff and the Class have suffered irreparable harm and damages because of
21 Defendants' wrongful conduct as alleged herein. Absent certification, Plaintiff and the Class will
22 continue to be damaged and to suffer by the unauthorized disclosure and/or release of their medical
23 and personal identifying information, thereby allowing these violations of law to proceed without
24 remedy.

25 55. Moreover, Plaintiff's and the Class' individual damages are insufficient to justify the
26 cost of litigation, so that in the absence of class treatment, Defendants' violations of law inflicting
27 substantial damages in the aggregate would go unremedied. In addition, Defendants have acted or
28

1 refused to act on grounds generally applicable to Plaintiff and the Class, thereby making appropriate
2 final injunctive relief with respect to, the Class as a whole.

3 **FIRST CAUSE OF ACTION**
4 **Violations of the Confidentiality of Medical Information Act**
5 **California Civil Code §§ 56, et seq.**
6 **(On Behalf of Plaintiff and the Class All Defendants)**

7 56. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
8 fully stated herein.

9 57. At all times relevant to this action, including prior to and in December 2020,
10 Defendants are providers of health care, contractors, and/or other authorized recipients of personal
11 and confidential medical information as defined and set forth in the California Confidentiality of
12 Medical Information Act, California Civil Code §§ 56, *et seq.* (the “Act”) and maintained and
13 continues to maintain “medical information,” within the meaning of Civil Code § 56.05(j), of
14 Plaintiff and other “patients” within the meaning of Civil Code § 56.05(k).

15 58. At all times relevant to this action, including prior to and in December 2020,
16 Defendants lawfully came into possession of Plaintiffs’ and Class members’ personally identifiable
17 medical information, including the names, dates of birth, medical diagnosis or treatment
18 information, health insurance information and/or client identification numbers of Plaintiff and the
19 Class, and had a duty to exercise reasonable care in preserving the confidentiality of this
20 information subject to the requirements and mandates of the Act, including but not limited to Civil
21 Code §§ 56.10, 56.13, 56.245, 56.26, 56.101 and 56.36. At all times relevant to this action,
22 including prior to and in December 2020, Plaintiff and the Class had their individually identifiable
23 “medical information,” within the meaning of Civil Code § 56.05(j), created, maintained, preserved,
24 and stored in SDFC’s email and computer network, including on SDFC’s information technology
25 hosting provider’s “systems that stored information.” Further, at all times relevant to this action,
26 including prior to and in December 2020, Plaintiff and the Class are “patients” within the meaning
27 of Civil Code § 56.05(k), and are “Endanger” within the meaning of Civil Code § 56.05(e) because
28 they fear that disclosure and/or release of their medical information could subject them to
harassment or abuse.

1 59. As a result, at all times relevant to this action, including prior to and in December
2 2020, Defendants and/or unknown employees negligently created, maintained, preserved, and/or
3 stored Plaintiff’s and the Class’ individual identifiable “medical information,” within the meaning
4 of Civil Code § 56.05(j), including Plaintiff’s and Class members’ names, dates of birth, medical
5 diagnosis or treatment information, health insurance information and/or client identification
6 numbers, in SDFC’s email and computer network, including on SDFC’s information technology
7 hosting provider’s “systems that stored information,” in a manner that did not preserve the
8 confidentiality of the information, and negligently failed to protect and preserve confidentiality of
9 electronic medical information of Plaintiff and the Class in its possession against disclosure and/or
10 release, including but not limited to, by failing to conduct and require adequate employee education
11 and training, failing to adequately review & revise information security, failing to have adequate
12 information security, and failing to have adequate privacy policies and procedures in place, as
13 required by the Act, under Civil Code §§ 56.10(a), 56.13, 56.245, 56.26(a), 56.101(a),
14 56.101(b)(1)(A), and 56.36(e)(2)(E).

15 60. Due to SDFC’s and/or its employees’ negligent creation, maintenance, preservation
16 and/or storage of Plaintiff’s and the Class’ electronic medical information in SDFC’s email and
17 computer network, including on SDFC’s information technology hosting provider’s “systems that
18 stored information,” SDFC allowed Plaintiff’s and the Class’ individually identifiable medical
19 information to be accessed and actually viewed by at least one unauthorized third party in
20 December 2020, without first obtaining an authorization within the meaning of Civil Code §
21 56.05(a), constituting a disclosure in violation of Civil Code §§ 56.10, 56.13, 56.245, and 56.26(a).

22 61. Due to SDFC’s and/or its employees’ negligent creation, maintenance, preservation
23 and/or storage of Plaintiff’s and the Class’ electronic medical information in SDFC’s email and
24 computer network, including on SDFC’s information technology hosting provider’s “systems that
25 stored information,” SDFC allowed Plaintiff’s and the Class’ individually identifiable medical
26 information to be accessed and actually viewed by at least one unauthorized third party in
27 December 2020, constituting a release in violation of Civil Code § 56.101(a).

28

1 62. Due to SDFC’s and/or its employees’ negligent creation, maintenance, preservation
2 and/or storage of Plaintiff’s and the Class’ electronic medical information in SDFC’s SDFC’s email
3 and computer network, including on SDFC’s information technology hosting provider’s “systems
4 that stored information,” SDFC allowed Plaintiff’s and the Class’ individually identifiable medical
5 information to be accessed and actually viewed by at least one unauthorized third party in
6 December 2020, constituting a release in violation of Civil Code § 56.101(b)(1)(A).

7 63. As a result of SDFC’s and/or its employees’ above-described conduct in violation
8 of the Act, Plaintiff and the Class have suffered damages from the unauthorized disclosure and/or
9 release of their individual identifiable medical information.

10 64. As a direct and proximate result of SDFC’s and/or its employees’ above-described
11 conduct in violation of the Act, Plaintiff and the Class are entitled to recover, “against any person or
12 entity who has negligently released confidential information or records concerning him or her in
13 violation of this part, for either or both of the following: (1) ... nominal damages of one thousand
14 dollars (\$1,000). In order to recover under this paragraph, it shall not be necessary that the plaintiff
15 suffered or was threatened with actual damages. (2) The amount of actual damages, if any,
16 sustained by the patient.”

17 65. As a result of SDFC’s and/or its employees’ above-described conduct in violation of
18 the Act, Plaintiff and the Class seek nominal damages of one thousand dollars (\$1,000) for each
19 violation under Civil Code §56.36(b)(1), and actual damages suffered, according to proof, for each
20 violation under Civil Code § 56.36(b)(2) from all Defendants.

21 **SECOND CAUSE OF ACTION**
22 **Breach of California Security Notification Laws**
 California Civil Code § 1798.82
23 **(On Behalf of Plaintiff and the Class Against All Defendants)**

24 66. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
25 fully stated herein.

26 67. Pursuant to Civil Code § 1798.82(a), “A person or business that conducts business in
27 California, and that owns or licenses computerized data that includes personal information, shall
28 disclose a breach of the security of the system following discovery or notification of the breach in

1 the security of the data to a resident of California (1) whose unencrypted personal information was,
2 or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted
3 personal information was, or is reasonably believed to have been, acquired by an unauthorized
4 person and the encryption key or security credential was, or is reasonably believed to have been,
5 acquired by an unauthorized person and the person or business that owns or licenses the encrypted
6 information has a reasonable belief that the encryption key or security credential could render that
7 personal information readable or usable. The disclosure shall be made in the most expedient time
8 possible and without unreasonable delay, consistent with the legitimate needs of law enforcement,
9 as provided in subdivision (c), or any measures necessary to determine the scope of the breach and
10 restore the reasonable integrity of the data system.” Prior to passage of such statute, the California
11 State Assembly cited an incident where authorities knew of the breach in security for 21 days
12 “before state workers were told” as an example of “late notice.”

13 68. Civil Code § 1798.82 further provides, “(h) For purposes of this section, ‘personal
14 information’ means an individual’s first name or first initial and last name in combination with any
15 one or more of the following data elements, when either the name or the data elements are not
16 encrypted: (1) Social security number. (2) Driver’s license number or California Identification Card
17 number. (3) Account number, credit or debit card number, in combination with any required
18 security code, access code, or password that would permit access to an individual’s financial
19 account. (4) Medical information. (5) Health insurance information. (i) (2) For purposes of this
20 section, ‘medical information’ means any information regarding an individual’s medical history,
21 mental or physical condition, or medical treatment or diagnosis by a health care professional. (3)
22 For purposes of this section, ‘health insurance information’ means an individual’s health insurance
23 policy number or subscriber identification number, any unique identifier used by a health insurer to
24 identify the individual, or any information in an individual’s application and claims history,
25 including any appeals records.”

26 69. SDFC conducts business in California and owns or licenses computerized data which
27 includes the personal information, within the meaning of Civil Code § 1798.82(h), of Plaintiff and
28 the Class.

1 70. Based upon SDFC’s form letter submitted to the Attorney General of the State of
2 California and mailed to Plaintiff and the Class attached hereto as **Exhibit A**, SDFC was aware that
3 Plaintiff’s and the Class’ unencrypted personal information was, or is reasonably believed to have
4 been, acquired by an unauthorized person no later than January 20, 2021, but did not begin to mail
5 notification letters to Plaintiff and the Class until May 7, 2021. Thus, SDFC waited at least 108
6 days before *beginning* to inform Plaintiff and the Class of this incident and the subsequent threat to
7 Plaintiff’s and the Class’ unencrypted personal information. As a result, SDFC did not disclose to
8 Plaintiff and the Class that their unencrypted personal information was, or was reasonably believed
9 to have been, acquired by an unauthorized person, in the most expedient time possible and without
10 reasonable delay in violation of Civil Code § 1798.82(a). Given the example of the Legislature
11 finding that a delay of 21 days to be “late notice” under the statute, SDFC’s delay of 108 days
12 before *beginning* to inform Plaintiff and the Class that their personal information was, or was
13 reasonably believed to have been, acquired by an unauthorized person by mailing SDFC’s form
14 letter to Plaintiff and the Class is presumptively unreasonable notice in violation of Civil Code §
15 1798.82(a).

16 71. Upon information and belief, Plaintiff believes and alleges that no law enforcement
17 agency has notified Defendants that the notification would impede a criminal investigation
18 justifying SDFC’s decision to wait 108 days *before beginning to mail* notification letters to Plaintiff
19 and the Class *after* they knew that Plaintiff’s and the Class’ unencrypted personal information on
20 SDFC’s email and computer server was, or was reasonably believed to have been, acquired by an
21 “unauthorized individual.” Upon information and belief, Plaintiff believes and alleges that there
22 were no measures taken by SDFC to determine the scope of the breach or to restore the reasonable
23 integrity of the data system, which justifies SDFC’s decision to wait 108 days *before beginning to*
24 *mail* notification letters to Plaintiff and the Class. Moreover, SDFC’s notification letter mailed to
25 Plaintiff and the Class failed to state whether notification was delayed as a result of a law
26 enforcement investigation, in violation of Civil Code § 1798.82(d)(2)(D).

27 72. Additionally, SDFC’s notification letter mailed to Plaintiff and the Class failed to
28 provide with the requisite specificity either (i) the date of the breach, (ii) the estimated date of the

1 breach, or (iii) the date range within which the breach occurred, in violation of Civil Code §
2 1798.82(d)(2)(C).

3 73. Plaintiff and the Class have been injured by fact that Defendants did not disclose to
4 them that their unencrypted personal information was, or was reasonably believed to have been,
5 acquired by an unauthorized person in the most expedient time possible and without reasonable
6 delay in violation of Civil Code § 1798.82(a). Defendants' delays in informing required by Civil
7 Code § 1798.82(a) and providing all of the information required by Civil Code § 1798.82(d) to
8 Plaintiff and the Class that their unencrypted personal information was, or was reasonably believed
9 to have been, acquired by an unauthorized person, have prevented Plaintiff and the Class from
10 taking steps in the most expedient time possible to protect their unencrypted personal information
11 from unauthorized use and/or identify theft.

12 74. Plaintiff and the Class seek recovery of their damages pursuant to Civil Code §
13 1798.84(b) and injunctive relief pursuant to Civil Code § 1798.84(e) from all Defendants.

14 **THIRD CAUSE OF ACTION**
15 **Unlawful and Unfair Business Acts and Practices in Violation of**
16 **California Business & Professions Code §17200, *et seq.***
(On Behalf of Plaintiff and the Class Against All Defendants)

17 75. Plaintiff incorporates by reference all of the above paragraphs of this complaint as if
18 fully stated herein.

19 76. The acts, misrepresentations, omissions, practices, and non-disclosures of
20 Defendants as alleged herein constituted unlawful and unfair business acts and practices within the
21 meaning of California Business & Professions Code §§ 17200, *et seq.*

22 77. By the aforementioned business acts or practices, Defendants have engaged in
23 "unlawful" business acts and practices in violation of the aforementioned statutes, including Civil
24 Code §§ 56.10(a), 56.26(a), 56.36(e)(2)(E), 56.101(a), 56.101(b)(1)(A), 1798.82(a) and 1798.82(d).
25 Plaintiff reserves the right to allege other violations of law committed by Defendants which
26 constitute unlawful acts or practices within the meaning of California Business & Professions Code
27 §§ 17200, *et seq.*

1 78. By the aforementioned business acts or practices, Defendants have also engaged in
2 “unfair” business acts or practices in that the harm caused by Defendants’ failure to maintain
3 adequate information security procedures and practices, including but not limited to, failing to take
4 adequate and reasonable measures to ensure its data systems were protected against unauthorized
5 intrusions, failing to properly and adequately educate and train its employees, failing to put into
6 place reasonable or adequately computer systems and security practices to safeguard patients’
7 identifiable medical information including access restrictions and encryption, failing to have
8 adequate privacy policies and procedures in place that did not preserve the confidentiality of the
9 medical and personal identifying information of Plaintiff and the Class in their possession, and
10 failing to protect and preserve confidentiality of electronic medical information of Plaintiff and the
11 Class in their possession against disclosure and/or release, outweighs the utility of such conduct and
12 such conduct offends public policy, is immoral, unscrupulous, unethical, deceitful and offensive,
13 and causes substantial injury to Plaintiff and the Class.

14 79. Defendants have obtain money and property from Plaintiff and the Class because of
15 the payment of the services and products they received from Defendants. Plaintiff and the Class
16 have suffered an injury in fact by acquiring less in their transactions with Defendants for the
17 services and products they received from Defendants than they otherwise would have if Defendants
18 would had adequately protected the confidentiality of their medical and personal identifying
19 information.

20 80. Pursuant to the Business & Professions Code § 17203, Plaintiff and the Class seek an
21 order of this Court requiring Defendants awarding Plaintiff and the Class restitution of monies
22 wrongfully acquired by Defendants in the form of payments for services by means of such
23 unlawful, fraudulent and unfair business acts and practices, so as to restore any and all monies to
24 Plaintiff and the Class which were acquired and obtained by means of such unlawful, fraudulent and
25 unfair business acts and practices, which ill-gotten gains are still retained by Defendants.

26 81. The aforementioned unlawful, fraudulent and unfair business acts or practices
27 conducted by Defendants have been committed in the past and continues to this day. Defendants
28 have failed to acknowledge the wrongful nature of their actions. Defendants have not corrected or

1 publicly issued comprehensive corrective notices to Plaintiff and the Class, and have not corrected
2 or enacted adequate privacy policies and procedures to protect and preserve confidentiality of
3 medical and personal identifying information of Plaintiff and the Class in their possession.

4 82. Because of Defendants' aforementioned conduct, Plaintiff and the Class have no
5 other adequate remedy of law in that absent injunctive relief from the Court and Defendants are
6 likely to continue to injure Plaintiff and the Class.

7 83. Pursuant to Business & Professions Code § 17203, Plaintiff and the Class also seek
8 an order of this Court for equitable and/or injunctive relief in the form of requiring Defendants to
9 correct its illegal conduct that is necessary and proper to prevent Defendants from repeating their
10 illegal and wrongful practices as alleged above and protect and preserve confidentiality of medical
11 and personal identifying information of Plaintiff and the Class in Defendants' possession that has
12 already been accessed, acquired, exfiltrated, stolen and viewed by at least one unauthorized third
13 party because by way of Defendants' illegal and wrongful practices set forth above. Pursuant to
14 Business & Professions Code § 17203, Plaintiff and the Class further seek an order of this Court for
15 equitable and/or injunctive relief in the form of requiring Defendants to publicly issue
16 comprehensive corrective notices.

17 84. Because this case is brought for the purposes of enforcing important rights affecting
18 the public interest, Plaintiff and the Class also seek the recovery of attorneys' fees and costs in
19 prosecuting this action against Defendants under Code of Civil Procedure § 1021.5 and other
20 applicable law.

21 **PRAYER FOR RELIEF**

22 WHEREFORE, Plaintiff respectfully request that the Court grant Plaintiff and the proposed
23 Class the following relief against Defendants, and each of them:

24 **As for the First Cause of Action**

- 25 1. For nominal damages in the amount of one thousand dollar (\$1,000) per violation to Plaintiff
26 individually and to each member of the Class and the Class pursuant to Civil Code §
27 56.36(b)(1);
28 2. For actual damages according to proof per violation pursuant to Civil Code § 56.36(b)(2);

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

As for the Second Cause of Action

- 3. For damages according to proof to Plaintiff individually and to each member of the Class and the Class pursuant to California Civil Code § 1798.84(b);
- 4. For injunctive relief pursuant to California Civil Code § 1798.84(e);

As for the Third Cause of Action


- 5. For an order awarding Plaintiff and the Class restitution of all monies wrongfully acquired by Defendants by means of such unlawful, fraudulent and unfair business acts and practices;
- 6. For injunctive relief in the form of an order instructing Defendants to prohibit the unauthorized release of medical and personal identifying information of Plaintiff and the Class, and to adequately maintain the confidentiality of the medical and personal identifying information of Plaintiff and the Class;
- 7. For injunctive relief in the form of an order enjoining Defendants from disclosing the medical and personal identifying information of Plaintiff and the Class without the prior written authorization of each Plaintiff and the Class member;

As to All Causes of Action

- 8. That the Court issue an Order certifying this action be certified as a class action on behalf of the proposed Class, appointing Plaintiff as representative of the proposed Class, and appointing Plaintiff’s attorneys, as counsel for members of the proposed Class;
- 9. For an award of attorneys’ fees as authorized by statute, including, but not limited to, the provisions of California Code of Civil Procedure § 1021.5, and as authorized under the “common fund” doctrine, and as authorized by the “substantial benefit” doctrine;
- 10. For costs of the suit;
- 11. For prejudgment interest at the legal rate; and
- 12. Any such further relief as this Court deems necessary, just, and proper.

Dated: May 25, 2021

KEEGAN & BAKER LLP

By: 
 Patrick N. Keegan, Esq.
 Attorney for Plaintiff

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DEMAND FOR JURY TRIAL

Plaintiff and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

Dated: May 25, 2021

KEEGAN & BAKER LLP


By: 
Patrick N. Keegan, Esq.
Attorney for Plaintiff

Exhibit A



SAN DIEGO FAMILY CARE
A California Non-Profit Corporation

C/O IDX

P.O. Box 989728

West Sacramento, CA 95798-9728

To Enroll, Please Call:

(833) 664-1997

Or Visit:

<https://response.idx.us/sdfcprotect>

Enrollment Code: <<XXXXXX>>

<<FIRST NAME>> <<LAST NAME>>

<<ADDRESS1>>

<<ADDRESS2>>

<<CITY>>, <<STATE>> <<ZIP>>

May 7, 2021

Subject: Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>:

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 <<Variable 2>>.

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

What You Can Do. We recommend that you review the guidance included with this letter about how to protect your information. In addition, you can enroll in the free credit monitoring services that we are offering to you through IDX by calling (833) 664-1997 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, 6am – 6pm PT. Our representatives are fully versed on this incident and can answer any questions you may have regarding the protection 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 this may cause you.

Sincerely,

Roberta L. Feinberg, M.S.

Chief Executive Officer

San Diego Family Care

<<Nombre>> <<Apellido>>
<<Dirección1>>
<<Dirección2>>
<<Ciudad>>, <<Estado>> <<Código postal>>

Para inscribirse, llame al:
(833) 664-1997
o visite:
<https://response.idx.us/sdfcprotect>
Código de inscripción: <<xxxxxx>>

Asunto: Aviso de incidente de seguridad de datos

7 de mayo de 2021

Estimado/a <<Nombre>> <<Apellido>>:

Le escribo para informarle acerca de un incidente de seguridad de datos que puede haber afectado su información personal. En San Diego Family Care (SDFC), nos tomamos muy en serio la privacidad y seguridad de su información personal. Nos comunicamos con usted para informarle la existencia de este incidente y las medidas que puede tomar para asegurarse de que su información esté protegida, incluida la inscripción en los servicios complementarios de protección de identidad que ponemos a su disposición.

Qué ocurrió. En diciembre de 2020, SDFC y su socio comercial, Health Center Partners of Southern California (HCP), tuvieron conocimiento de que nuestro proveedor de hosting de tecnología de la información experimentó un incidente de seguridad de datos que dio como resultado el cifrado de cierta información. El proveedor de hosting tomó medidas para proteger y restaurar sus sistemas e inició una investigación con la ayuda de expertos en informática forense. En ese momento, SDFC no sabía qué datos de SDFC o HCP, en caso de que existiera alguno, podrían haber estado involucrados en el incidente.

El 20 de enero de 2021, nos enteramos de que, según la investigación de nuestro proveedor de hosting sobre el incidente, es posible que una persona no autorizada haya accedido o adquirido ciertos datos de SDFC. Obtuvimos una copia de los datos afectados y contratamos a expertos para realizar una revisión exhaustiva a fin de identificar a las personas cuya información puede haber estado involucrada en el incidente. Dicha revisión concluyó el 12 de abril de 2021 e indicó que su información puede haber estado involucrada.

Tenga en cuenta que este acceso no autorizado se limitó a sistemas que almacenaban información sobre reclamaciones de seguros y no afectó a ningún otro sistema de información de SDFC, como nuestro sistema de registro médico electrónico. No tenemos conocimiento del uso indebido de ninguna información personal que pueda haber sido afectada por este incidente.

Qué información estuvo involucrada. La información afectada incluye nombres de personas, números de seguro social, fechas de nacimiento, diagnósticos médicos o información sobre tratamientos, información del seguro médico o números de identificación de clientes. Sin embargo, no todos los elementos de los datos se vieron afectados para cada persona. Puede encontrar información adicional en la página 1 o al llamar al (833) 664-1997.

Medidas que tomamos. Tan pronto como SDFC tuvo conocimiento del incidente, tomamos las medidas descritas anteriormente. También estamos trabajando con nuestro proveedor de hosting para asegurarnos de que se tomen las medidas correctivas adecuadas para reducir la probabilidad de que ocurra un incidente similar en el futuro. Además, ofrecemos servicios de protección contra robo de identidad a través de IDX, el experto en servicios de violación y recuperación de datos. Los servicios de protección de identidad de IDX incluyen: 12 meses de supervisión de crédito y CyberScan, una política de reembolso de \$1,000,000 en concepto de seguro y servicios de recuperación de robo de identidad completamente administrados. Con esta protección, IDX lo ayudará a resolver problemas si su identidad está comprometida.

Qué puede hacer usted Le recomendamos que revise la orientación incluida con esta carta sobre cómo proteger su información. Además, para inscribirse en los servicios gratuitos de supervisión de crédito que le ofrecemos a través de IDX, puede llamar al (833) 664-1997 o visitar <https://response.idx.us/sdfcprotect> y usar el Código de inscripción proporcionado anteriormente.

Más información. Si tiene preguntas o necesita ayuda, comuníquese con el (833) 664-1997, de lunes a viernes, de 6 a. m. a 6 p. m., Hora del Pacífico. Nuestros representantes están plenamente informados sobre este incidente y pueden responder cualquier pregunta que pueda tener con respecto a la protección de su información personal.

Nos tomamos muy en serio su confianza y este asunto. Acepte nuestras más sinceras disculpas por cualquier preocupación o inconveniente que esto pueda ocasionarle.

Atentamente.



Roberta L. Feinberg, M.S.
Directora Ejecutiva
San Diego Family Care

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com
---	--	--	--

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is: Federal Trade Commission, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov or www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, Rhode Island, and the District of Columbia can obtain more information from their Attorneys General using the contact information below.

New York Attorney General Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI, 02903 riag.ri.gov 1-401-274-4400	District of Columbia Attorney General 400 6 th Street NW Washington, D.C., 20001 http://www.oag.dc.gov 202-727-3400
---	--	--	---	--

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three national credit reporting agencies may be found above.

MEDIDAS QUE PUEDE TOMAR PARA PROTEGER AÚN MÁS SU INFORMACIÓN

Revise sus estados de cuenta y notifique actividades sospechosas a las autoridades policiales: Como medida de precaución, le recomendamos que se mantenga alerta y revise atentamente sus estados de cuenta e informes de crédito. Si detecta alguna actividad sospechosa en una cuenta, debe notificar de inmediato a la empresa o institución financiera con la que se mantiene la cuenta. También debe informar de inmediato cualquier actividad fraudulenta o cualquier sospecha de robo de identidad a las autoridades policiales correspondientes, al Fiscal General de su estado y a la Comisión Federal de Comercio (la "FTC").

Copia del informe crediticio Para obtener una copia gratuita de su informe crediticio por parte de cada una de las tres principales agencias de informes de crédito una vez cada 12 meses, visite <http://www.annualcreditreport.com/>, llame a la línea gratuita 877-322-8228, o complete un Formulario de solicitud de informe crediticio anual y envíelo por correo al Servicio de solicitud de informe crediticio anual, P.O. Box 105281, Atlanta, GA 30348. También puede ponerse en contacto con una de las tres siguientes agencias nacionales de informes de crédito:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com
---	--	--	--

Alerta de fraude: Es posible que considere colocar una alerta de fraude en su informe crediticio. Una alerta de fraude inicial es gratuita y permanecerá en su archivo de crédito durante al menos 90 días. La alerta informa a los acreedores posibles actividades fraudulentas dentro de su informe y solicita que el acreedor se comunique con usted antes de establecer cuentas a su nombre. Para colocar una alerta de fraude en su informe crediticio, comuníquese con cualquiera de las tres agencias de informes de crédito identificadas anteriormente. Puede encontrar información adicional en <http://www.annualcreditreport.com>.

Congelamiento de seguridad: Tiene derecho a aplicar un congelamiento de seguridad en su archivo de crédito. Esto evitará que se abra un crédito nuevo a su nombre sin el uso de un número PIN que se le emite cuando inicia el congelamiento. Un congelamiento de seguridad está diseñado para evitar que potenciales acreedores accedan a su informe crediticio sin su consentimiento. Como resultado, la utilización de un congelamiento de seguridad puede interferir con o demorar su capacidad para obtener crédito. Debe colocar un congelamiento de seguridad en su archivo de crédito por separado con cada agencia de informes de crédito. Colocar, levantar o quitar un congelamiento de seguridad no tienen ningún costo. Para colocar un congelamiento de seguridad, es posible que deba proporcionar a la agencia de informes del consumidor información que lo identifique, incluido su nombre completo, número de seguro social, fecha de nacimiento, direcciones actuales y anteriores, una copia de su tarjeta de identificación emitida por el estado y una factura de servicios públicos, un extracto bancario o un extracto de seguro recientes.

Recursos gratuitos adicionales: Puede obtener información de las agencias de informes del consumidor, la FTC o el Fiscal General de su respectivo estado sobre alertas de fraude, congelamientos de seguridad y medidas que puede tomar para prevenir el robo de identidad. Puede denunciar la sospecha de robo de identidad a las autoridades policiales locales, incluso a la FTC o al Fiscal General de su estado. La información de contacto de la FTC es: Federal Trade Commission (Comisión Federal de Comercio), 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov o www.ftc.gov/idtheft, 1-877-438-4338. Los residentes de Nueva York, Maryland, Carolina del Norte y Rhode Island pueden obtener más información de sus Fiscales Generales a través de la información de contacto a continuación.

New York Attorney General (Fiscal General de Nueva York) Bureau of Internet and Technology Resources 28 Liberty Street Nueva York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	Maryland Attorney General (Fiscal General de Maryland) 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General (Fiscal General de Carolina del Norte) 9001 Centro de servicio de correo Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General (Fiscal General de Rhode Island) 150 South Main Street Providence, RI, 02903 riag.ri.gov 1-401-274-4400	District of Columbia Attorney General (Fiscal General del Distrito de Columbia) 400 6 th Street NW Washington, D.C., 20001 http://www.oag.dc.gov 202-727-3400
--	---	--	--	--

También tiene otros derechos conforme a la Ley de Informe Imparcial de Crédito (FCRA, por sus siglas en inglés): Estos derechos incluyen el derecho a saber qué hay en su archivo; debatir información incompleta o inexacta; y solicitar a las agencias de informes del consumidor que corrijan o eliminen información inexacta, incompleta o no verificable. Para obtener más información sobre la FCRA, visite <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Información personal de un menor: Puede solicitar que cada una de las tres agencias nacionales de informes de crédito realice una búsqueda manual del número de seguro social de un menor para determinar si existe un informe de crédito asociado. Es posible que se requieran copias de la información de identificación del menor y del padre/tutor, incluido el certificado de nacimiento o adopción, la tarjeta del Seguro Social y la tarjeta de identificación emitida por el gobierno. Si existe un informe de crédito, debe solicitar una copia del informe y comunicar de inmediato cualquier cuenta fraudulenta a la agencia de informes de crédito. También puede denunciar cualquier uso indebido de la información de un menor a la FTC en <https://www.identitytheft.gov/>. Para obtener más información sobre el robo de identidad infantil e instrucciones para solicitar una búsqueda manual de número de seguro social, visite el sitio web de la FTC: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. La información de contacto de las tres agencias nacionales de informes de crédito se puede encontrar más arriba.



SAN DIEGO FAMILY CARE
A California Non-Profit Corporation

C/O IDX

P.O. Box 989728

West Sacramento, CA 95798-9728

<<FIRST NAME>> <<LAST NAME>>

<<ADDRESS1>>

<<ADDRESS2>>

<<CITY>>, <<STATE>> <<ZIP>>

May 7, 2021

Subject: Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>:

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.

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 <<Variable 2>>.

What Are We Doing. As soon as SDFC learned of the incident, we took the steps described above. We are also working with our hosting provider to ensure that appropriate remediation measures are taken to reduce the likelihood of a similar incident occurring in the future.

What You Can Do. We recommend that you review the guidance included with this letter about how to protect your information.

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

Sincerely,

Roberta L. Feinberg, M.S.

Chief Executive Officer

San Diego Family Care

<<Nombre>> <<Apellido>>
<<Dirección1>>
<<Dirección2>>
<<Ciudad>>, <<Estado>> <<Código postal>>

7 de mayo de 2021

Asunto: Aviso de incidente de seguridad de datos

Estimado/a <<Nombre>> <<Apellido>>:

Le escribo para informarle acerca de un incidente de seguridad de datos que puede haber afectado su información personal. En San Diego Family Care ("SDFC"), nos tomamos muy en serio la privacidad y seguridad de su información personal. Nos comunicamos con usted para informarle la existencia de este incidente y las medidas que puede tomar para asegurarse de que su información esté protegida.

Qué ocurrió. En diciembre de 2020, SDFC y su socio comercial, Health Center Partners of Southern California (HCP), tuvieron conocimiento de que nuestro proveedor de hosting de tecnología de la información experimentó un incidente de seguridad de datos que dio como resultado el cifrado de cierta información. El proveedor de hosting tomó medidas para proteger y restaurar sus sistemas e inició una investigación con la ayuda de expertos en informática forense. En ese momento, SDFC no sabía qué datos de SDFC o HCP, en caso de que existiera alguno, podrían haber estado involucrados en el incidente.

El 20 de enero de 2021, nos enteramos de que, según la investigación de nuestro proveedor de hosting sobre el incidente, es posible que una persona no autorizada haya accedido o adquirido ciertos datos de SDFC. Obtuvimos una copia de los datos afectados y contratamos a expertos para realizar una revisión exhaustiva a fin de identificar a las personas cuya información puede haber estado involucrada en el incidente. Dicha revisión concluyó el 12 de abril de 2021 e indicó que su información puede haber estado involucrada.

Tenga en cuenta que este acceso no autorizado se limitó a sistemas que almacenaban información sobre reclamaciones de seguros y no afectó a ningún otro sistema de información de SDFC, como nuestro sistema de registro médico electrónico. No tenemos conocimiento del uso indebido de ninguna información personal que pueda haber sido afectada por este incidente.

Qué información estuvo involucrada. La información afectada incluye nombres de personas, fechas de nacimiento, diagnósticos médicos o información sobre tratamientos, información del seguro médico o números de identificación de clientes. Sin embargo, no todos los elementos de los datos se vieron afectados para cada persona. Puede encontrar información adicional en la página 1 o al llamar al (833) 664-1997.

Medidas que tomamos. Tan pronto como SDFC tuvo conocimiento del incidente, tomamos las medidas descritas anteriormente. También estamos trabajando con nuestro proveedor de hosting para asegurarnos de que se tomen las medidas correctivas adecuadas para reducir la probabilidad de que ocurra un incidente similar en el futuro.

Qué puede hacer usted Le recomendamos que revise la orientación incluida con esta carta sobre cómo proteger su información.

Más información. Si tiene preguntas o necesita ayuda, comuníquese con el (833) 664-1997, de lunes a viernes, de 6 a. m. a 6 p. m., Hora del Pacífico. Nuestros representantes están plenamente informados sobre este incidente y pueden responder cualquier pregunta que pueda tener con respecto a la protección de su información personal.

Nos tomamos muy en serio su confianza y este asunto. Acepte nuestras más sinceras disculpas por cualquier preocupación o inconveniente que esto pueda ocasionarle.

Atentamente.



Roberta L. Feinberg, M.S.
Directora Ejecutiva
San Diego Family Care

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com
---	--	--	--

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is: Federal Trade Commission, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov or www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, Rhode Island, and the District of Columbia can obtain more information from their Attorneys General using the contact information below.

New York Attorney General Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI, 02903 riag.ri.gov 1-401-274-4400	District of Columbia Attorney General 400 6 th Street NW Washington, D.C., 20001 http://www.oag.dc.gov 202-727-3400
---	--	--	---	--

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three national credit reporting agencies may be found above.

MEDIDAS QUE PUEDE TOMAR PARA PROTEGER AÚN MÁS SU INFORMACIÓN

Revise sus estados de cuenta y notifique actividades sospechosas a las autoridades policiales: Como medida de precaución, le recomendamos que se mantenga alerta y revise atentamente sus estados de cuenta e informes de crédito. Si detecta alguna actividad sospechosa en una cuenta, debe notificar de inmediato a la empresa o institución financiera con la que se mantiene la cuenta. También debe informar de inmediato cualquier actividad fraudulenta o cualquier sospecha de robo de identidad a las autoridades policiales correspondientes, al Fiscal General de su estado y a la Comisión Federal de Comercio (la "FTC").

Copia del informe crediticio Para obtener una copia gratuita de su informe crediticio por parte de cada una de las tres principales agencias de informes de crédito una vez cada 12 meses, visite <http://www.annualcreditreport.com/>, llame a la línea gratuita 877-322-8228, o complete un Formulario de solicitud de informe crediticio anual y envíelo por correo al Servicio de solicitud de informe crediticio anual, P.O. Box 105281, Atlanta, GA 30348. También puede ponerse en contacto con una de las tres siguientes agencias nacionales de informes de crédito:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com
---	--	--	--

Alerta de fraude: Es posible que considere colocar una alerta de fraude en su informe crediticio. Una alerta de fraude inicial es gratuita y permanecerá en su archivo de crédito durante al menos 90 días. La alerta informa a los acreedores posibles actividades fraudulentas dentro de su informe y solicita que el acreedor se comunique con usted antes de establecer cuentas a su nombre. Para colocar una alerta de fraude en su informe crediticio, comuníquese con cualquiera de las tres agencias de informes de crédito identificadas anteriormente. Puede encontrar información adicional en <http://www.annualcreditreport.com>.

Congelamiento de seguridad: Tiene derecho a aplicar un congelamiento de seguridad en su archivo de crédito. Esto evitará que se abra un crédito nuevo a su nombre sin el uso de un número PIN que se le emite cuando inicia el congelamiento. Un congelamiento de seguridad está diseñado para evitar que potenciales acreedores accedan a su informe crediticio sin su consentimiento. Como resultado, la utilización de un congelamiento de seguridad puede interferir con o demorar su capacidad para obtener crédito. Debe colocar un congelamiento de seguridad en su archivo de crédito por separado con cada agencia de informes de crédito. Colocar, levantar o quitar un congelamiento de seguridad no tienen ningún costo. Para colocar un congelamiento de seguridad, es posible que deba proporcionar a la agencia de informes del consumidor información que lo identifique, incluido su nombre completo, número de seguro social, fecha de nacimiento, direcciones actuales y anteriores, una copia de su tarjeta de identificación emitida por el estado y una factura de servicios públicos, un extracto bancario o un extracto de seguro recientes.

Recursos gratuitos adicionales: Puede obtener información de las agencias de informes del consumidor, la FTC o el Fiscal General de su respectivo estado sobre alertas de fraude, congelamientos de seguridad y medidas que puede tomar para prevenir el robo de identidad. Puede denunciar la sospecha de robo de identidad a las autoridades policiales locales, incluso a la FTC o al Fiscal General de su estado. La información de contacto de la FTC es: Federal Trade Commission (Comisión Federal de Comercio), 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov o www.ftc.gov/idtheft, 1-877-438-4338. Los residentes de Nueva York, Maryland, Carolina del Norte y Rhode Island pueden obtener más información de sus Fiscales Generales a través de la información de contacto a continuación.

New York Attorney General (Fiscal General de Nueva York) Bureau of Internet and Technology Resources 28 Liberty Street Nueva York, NY 10005 ifraud@ag.ny.gov 1-212-416-8433	Maryland Attorney General (Fiscal General de Maryland) 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General (Fiscal General de Carolina del Norte) 9001 Centro de servicio de correo Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General (Fiscal General de Rhode Island) 150 South Main Street Providence, RI, 02903 riag.ri.gov 1-401-274-4400	District of Columbia Attorney General (Fiscal General del Distrito de Columbia) 400 6 th Street NW Washington, D.C., 20001 http://www.oag.dc.gov 202-727-3400
--	---	--	--	--

También tiene otros derechos conforme a la Ley de Informe Imparcial de Crédito (FCRA, por sus siglas en inglés): Estos derechos incluyen el derecho a saber qué hay en su archivo; debatir información incompleta o inexacta; y solicitar a las agencias de informes del consumidor que corrijan o eliminen información inexacta, incompleta o no verificable. Para obtener más información sobre la FCRA, visite <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Información personal de un menor: Puede solicitar que cada una de las tres agencias nacionales de informes de crédito realice una búsqueda manual del número de seguro social de un menor para determinar si existe un informe de crédito asociado. Es posible que se requieran copias de la información de identificación del menor y del padre/tutor, incluido el certificado de nacimiento o adopción, la tarjeta del Seguro Social y la tarjeta de identificación emitida por el gobierno. Si existe un informe de crédito, debe solicitar una copia del informe y comunicar de inmediato cualquier cuenta fraudulenta a la agencia de informes de crédito. También puede denunciar cualquier uso indebido de la información de un menor a la FTC en <https://www.identitytheft.gov/>. Para obtener más información sobre el robo de identidad infantil e instrucciones para solicitar una búsqueda manual de número de seguro social, visite el sitio web de la FTC: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. La información de contacto de las tres agencias nacionales de informes de crédito se puede encontrar más arriba.