

1 Tina Wolfson (SBN 174806)
2 *twolfson@ahdootwolfson.com*
3 Bradley K. King (SBN 274399)
4 *bking@ahdootwolfson.com*
5 **AHDOOT & WOLFSON, PC**
6 10728 Lindbrook Drive
7 Los Angeles, CA 90024
8 Tel: (310) 474-9111
9 Fax: (310) 474-8585

6 Cornelius P. Dukelow*
7 Oklahoma Bar No. 19086
8 **ABINGTON COLE + ELLERY**
9 320 South Boston Avenue
10 Suite 1130
11 Tulsa, Oklahoma 74103
12 918.588.3400 (*telephone & facsimile*)
13 *cdukelow@abingtonlaw.com*

11 *Pro Hac Vice application to be submitted

12 *Counsel for Plaintiff*

13 **UNITED STATES DISTRICT COURT**
14 **CENTRAL DISTRICT OF CALIFORNIA**

15 HECTOR FUENTES, individually and
16 on behalf of all others similarly situated,

17 Plaintiff,

18 v.

19 SUNSHINE BEHAVIORAL HEALTH
20 GROUP LLC,

21 Defendant.

Case No. 8:20-cv-00487

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiff, Hector Fuentes (“Plaintiff”), individually and on behalf of all others similarly
2 situated, alleges the following against Defendant Sunshine Behavioral Health Group LLC
3 (“Defendant”) based upon personal knowledge with respect to himself and on information
4 and belief derived from, among other things, investigation of counsel and review of public
5 documents as to all other matters:

6 **BRIEF SUMMARY OF THE CASE**

7 1. Defendant operates luxury drug and alcohol addiction rehabilitation facilities
8 in California, Colorado, and Texas.

9 2. On September 4, 2019, Defendant learned it was experiencing a data breach
10 (the “Data Breach”) resulting in the exposure and exfiltration of sensitive personal and
11 medical information of approximately 3,500 patients (“Affected Patients”).

12 3. The Affected Patients’ data exposed by Defendant and exfiltrated in the Data
13 Breach included the types of information that federal and state law requires companies to
14 take security measures to protect: names, addresses, credit card numbers, debit card
15 numbers, expiration dates, security codes, electronic or digital signatures, insurance carriers,
16 insurance membership numbers, insurance policy numbers, account balance information,
17 clinical information, medical information, and Social Security numbers (“Personal and
18 Medical Information”). This data should have received the most rigorous protection
19 available – it did not.

20 4. Even though Defendant was storing sensitive Personal and Medical
21 Information that it knew was valuable to criminals, and vulnerable to exfiltration, Defendant
22 failed to take security precautions necessary to protect Affected Patients’ data. Because
23 Defendant failed to take necessary security precautions, Affected Patients’ Personal and
24 Medical Information was viewable online and exfiltrated. Additionally, due to a webpage
25 setting that permitted search engines to index internal webpages that Defendant uses for
26 business operations, Affected Patients’ Personal and Medical Information was also
27 searchable, findable, viewable, and downloadable by anyone with access to an internet search
28 engine such as Google, Yahoo, Bing, etc.

PARTIES

1
2 5. Plaintiff Hector Fuentes is an individual residing in East Stroudsburg,
3 Pennsylvania. Mr. Fuentes was one of Defendant’s patients from January 17, 2019 to
4 February 17, 2019. Defendant received and collected Mr. Fuentes’ Personal and Medical
5 Information, which Defendant maintained in its computer systems. In January 2020, Mr.
6 Fuentes received a letter dated January 21, 2020, from Defendant informing him that his
7 Personal and Medical Information was compromised as a result of the Data Breach. Since
8 the Data Breach, someone has attempted to fraudulently open a credit card in Mr. Fuentes’
9 name. Since the Data Breach, Mr. Fuentes has begun receiving magazine subscriptions in his
10 name that he did not purchase and receiving invoices for those magazine subscriptions. Since
11 learning of the Data Breach, Mr. Fuentes has become worried that he will become a victim
12 of identity theft or other fraud which is causing him stress and anxiety. Since learning of the
13 Data Breach, Mr. Fuentes has spent in excess of 10 hours of his own time trying to make
14 sure he has not and does not become victimized because of the Data Breach.

15 6. Defendant Sunshine Behavioral Health Group LLC is a California limited
16 liability company with its principal place of business and headquarters in San Juan
17 Capistrano, California. (Discovery may reveal the following entities should be added as
18 defendants: Sunshine Behavioral Health LLC, Sunshine Behavioral Health Partners LLC,
19 and Itasca Holdings LLC.)

JURISDICTION AND VENUE

20
21 7. This Court has subject matter jurisdiction over this matter pursuant to 28
22 U.S.C. § 1332(d) because the amount in controversy exceeds \$5,000,000 (exclusive of
23 interests and costs), because there are more than 100 members in each of the proposed
24 classes, and because at least one member of each of the proposed classes is a citizen of a
25 State different from Defendant.

26 8. This Court has personal jurisdiction over Defendant because it is a California
27 limited liability company, is headquartered in California, and regularly conducts business in
28 California.

1 9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial
2 part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in, was
3 directed to, and/or emanated from this District.

4 **STATEMENT OF FACTS**

5 **Defendant**

6 10. Defendant is a drug and alcohol addiction rehabilitation business with facilities
7 in San Juan Capistrano, California, San Clemente, California, Monument, Colorado, and
8 Bastrop, Texas.

9 11. As part of its business, Defendant receives, collects, and maintains on its
10 computer systems a large amount of sensitive Personal and Medical Information, the
11 disclosure of which may be personally or professionally damaging for some individuals.
12 Moreover, given the nature of Defendant's business, the mere fact that an individual is or
13 was a patient at one of Defendant's facilities may be especially sensitive for some individuals
14 and disclosure of that fact alone may be personally or professionally damaging for some
15 individuals.

16 **The Data Breach**

17 12. On January 21, 2020, Defendant, for the first time, publicly admitted via a press
18 release ("Press Release") that it "recently experienced a privacy incident that affected the
19 protected health information of patients".¹

20 13. On January 21, 2020, Defendant also began filing with various state Attorneys
21 General sample "Notice of Data Breach" letters that mirrored the language of letters
22 Defendant began mailing to Affected Patients (including Plaintiff and Class Members) on or
23 about that same date. The Notice of Data Breach letter Defendant filed with the Attorney
24 General of California on January 21, 2020, is attached hereto as Exhibit 1.

25
26
27 ¹ *Privacy Incident* (January 21, 2020), [https://www.sunshinebehavioralhealth.com/privacy-](https://www.sunshinebehavioralhealth.com/privacy-incident/)
28 [incident/](https://www.sunshinebehavioralhealth.com/privacy-incident/) (last visited Mar. 5, 2020).

1 14. According to both the Press Release and the Notice of Data Breach, Defendant
2 first learned of the Data Breach on September 4, 2019.

3 15. Although the Press Release and Notice of Data Breach are both silent regarding
4 the date on which the Data Breach began, according to the California Attorney General, the
5 Data Breach began on March 1, 2017.² Thus, Defendant did not learn of the data breach
6 until 30 months after it began.

7 16. Furthermore, Defendant did not discover the Data Breach itself, but first
8 learned of the Data Breach after being notified by an individual not affiliated with Defendant.

9 17. According to both the Press Release and the Notice of Data Breach, “a cloud-
10 based system used to store certain patient records [] was inadvertently set-up in such a
11 manner that permitted the records to be made available on the Internet.”

12 18. According to both the Press Release and the Notice of Data Breach, Defendant
13 “immediately took steps to change the settings” after learning of the breach.

14 19. According to both the Press Release and the Notice of Data Breach, on
15 November 14, 2019, Defendant “took additional actions to remove the records from general
16 Internet access”.

17 20. On or about December 2, 2019, Defendant filed a notice with the U.S.
18 Department of Health and Human Services Office for Civil Rights indicating an
19 “Unauthorized Access/Disclosure” of protected health information of 3,500 individuals.

20 21. According to both the Press Release and the Notice of Data Breach, on
21 December 23, 2019, Defendant “determined that the incident potentially affected the
22 personal information of some patients [] and individuals who provided payment information
23 for these patients.”

24 22. Personal and Medical Information disclosed in the Data Breach included
25 Affected Patients’ first and last names, addresses, email addresses, demographic information,
26

27 ² *California Attorney General*, <https://oag.ca.gov/ecrime/databreach/reports/sb24-186209>
28 (last visited Mar. 5, 2020).

1 financial account information, credit and debit card numbers, credit and debit card expiration
2 dates, credit and debit card security codes, electronic or digital signatures, insurance carriers,
3 insurance membership numbers, insurance policy numbers, insurance claims information,
4 account balance information, clinical information, medical information, diagnostic codes,
5 treatment codes, and Social Security numbers.

6 23. Affected Patients' Personal and Medical Information described above was
7 exfiltrated during the Data Breach.

8 24. Defendant's Notice of Data Breach acknowledged the very real threat that the
9 incident would result in identity theft, fraud, and other similar risks by further informing
10 recipients of the notice – such as Plaintiff – to “remain vigilant by reviewing your account
11 statements and monitoring credit reports.”

12 25. Defendant's Notice of Data Breach advises victims that they may “report
13 suspected incidents of identity theft to local law enforcement or to the Attorney General”,
14 and that the “Federal Trade Commission also encourages those who discover that their
15 information has been misused to file a complaint with them.”

16 26. Defendant's Notice of Data Breach also explains to victims how to establish
17 fraud alerts with the three credit bureaus and establish credit security freezes.

18 27. Notably, to date, Defendant has not offered or provided to the victims any
19 fraud insurance. Instead, Defendant merely offered 24 months of credit monitoring services
20 to victims and provided victims with contact information for Experian, Transunion, and
21 Equifax as well as for the Federal Trade Commission-Consumer Response Center.
22 Defendant made general suggestions to contact local authorities and police, in addition to
23 suggestions on implementing a credit freeze if necessary. Essentially, all these steps are
24 mandated generalities used by virtually every company when publishing alerts about data
25 security breaches. Defendant failed to make any additional effort to mitigate or remediate
26 the damage caused by its failure to protect Affected Patients' Personal and Medical
27 Information.

1 28. Although Defendant knew of the Data Breach no later than September 4, 2019,
2 Defendant took no steps to notify Affected Patients until January 21, 2020, when Defendant
3 began mailing Notice of Data Breach letters to Affected Patients directly and until January
4 21, 2020, via Defendant's Press Release. This was a delay of 139 days.

5 **Defendant Expressly Promised to Protect Personal and Medical Information and**
6 **Acknowledged It is Required by Law to Protect Personal and Medical Information**

7 29. Defendant's Health Privacy Policy³ states, as relevant:

8 Your health record contains personal information about you and
9 your health. State and federal law protects the confidentiality of this
10 information. "Protected health information" is information about
11 you, including demographic information, that may identify you and
12 that relates to your past, present, or future physical or mental health
13 condition and related health care services. The confidentiality of
14 alcohol and drug abuse patient records is specifically protected by
15 Federal law and regulations. Sunshine Behavioral Health is required
16 to comply with these additional restrictions. This includes a
17 prohibition, with very few exceptions, on informing anyone outside
18 the program that you attend the program or disclosing any
19 information that identifies you as an alcohol or drug abuser. The
20 violation of Federal laws or regulations by this program is a crime.
21 If you suspect a violation you may file a report to the appropriate
22 authorities in accordance with Federal regulations.

23 ***

24 We are required by law to maintain the privacy of PHI and to
25 provide you with notice of Privacy Practices.

26
27 ³ *Sunshine Behavioral Health Privacy Policy*,
28 <https://www.sunshinebehavioralhealth.com/privacy/> (last visited Mar. 5, 2020).

1 30. Notwithstanding the foregoing assurances, promises, and obligations,
2 Defendant failed to protect the Personal and Medical Information of Plaintiff and other
3 Class Members, as conceded in the Defendant's Press Release and in Defendant's Notice of
4 Data Breach letters to Affected Patients.

5 31. If Defendant truly understood the importance of safeguarding Affected
6 Patients' Personal and Medical Information, it would acknowledge its responsibility for the
7 harm it has caused, and would compensate Class Members, provide long-term protection
8 for Plaintiff and Class Members, agree to Court-ordered and enforceable changes to its
9 cybersecurity policies and procedures, and adopt regular and intensive training to ensure that
10 a data breach like this never happens again.

11 32. Defendant's data security obligations were particularly important given the
12 known substantial increase in data breaches in the healthcare industry, including the recent
13 massive data breaches involving LabCorp, Quest Diagnostics, and American Medical
14 Collections Agency. And given the wide publicity given to these data breaches, there is no
15 excuse for Defendant's failure to adequately protect Plaintiff and Class Members' Personal
16 and Medical Information.

17 **Defendant had an Obligation to Protect Personal and Medical Information under**
18 **Federal and State Law and the Applicable Standard of Care**

19 33. Defendant had obligations created by HIPAA (42 U.S.C. § 1302d *et. seq.*),
20 California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56 *et seq.*),
21 California's Consumer Records Act (Cal. Civ. Code § 1798.82 *et seq.*) and based on industry
22 standards, to keep the compromised Personal and Medical Information confidential and to
23 protect it from unauthorized disclosures. Plaintiff and Class Members provided their
24 Personal and Medical Information to Defendant with the common sense understanding that
25 Defendant would comply with its obligations to keep such information confidential and
26 secure from unauthorized disclosures.

1 34. Defendant’s data security obligations and promises were particularly important
2 given the substantial increase in data breaches – particularly those in the healthcare industry
3 – which were widely known to the public and to anyone in Defendant’s industries.

4 35. Defendant is an entity covered by HIPAA (45 C.F.R. § 160.102). As such, it is
5 required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and
6 Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health
7 Information”), and Security Rule (“Security Standards for the Protection of Electronic
8 Protected Health Information), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

9 36. HIPAA’s Privacy Rule or *Standards for Privacy of Individually Identifiable Health*
10 *Information* establishes national standards for the protection of health information.

11 37. HIPAA’s Security Rule or *Security Standards for the Protection of Electronic Protected*
12 *Health Information* establishes a national set of security standards for protecting health
13 information that is maintained or transferred in electronic form.

14 38. HIPAA requires Defendant to “comply with the applicable standards,
15 implementation specifications, and requirements” of HIPAA “with respect to electronic
16 protected health information.” 45 C.F.R. § 164.302.

17 39. “Electronic protected health information” is “individually identifiable health
18 information . . . that is (i) Transmitted by electronic media; maintained in electronic media.”
19 45 C.F.R. § 160.103.

20 40. HIPAA’s Security Rule requires Defendant to do the following:

21 a. Ensure the confidentiality, integrity, and availability of all electronic
22 protected health information the covered entity or business associate creates, receives,
23 maintains, or transmits;

24 b. Protect against any reasonably anticipated threats or hazards to the
25 security or integrity of such information;

26 c. Protect against any reasonably anticipated uses or disclosures of such
27 information that are not permitted; and

28 d. Ensure compliance by its workforce.

1 41. HIPAA also required Defendant to “review and modify the security measures
2 implemented . . . as needed to continue provision of reasonable and appropriate protection
3 of electronic protected health information.” 45 C.F.R. § 164.306(e).

4 42. HIPAA also required Defendant to “[i]mplement technical policies and
5 procedures for electronic information systems that maintain electronic protected health
6 information to allow access only to those persons or software programs that have been
7 granted access rights.” 45 C.F.R. § 164.312(a)(1).

8 43. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required
9 Defendant to provide notice of the breach to each affected individual “without unreasonable
10 delay and *in no case later than 60 days following discovery of the breach.*”⁴

11 44. Defendant’s security failures demonstrate that it failed to honor its duties and
12 promises by not:

13 a. Maintaining an adequate data security system to reduce the risk of data
14 leaks, data breaches, and cyber-attacks;

15 b. Adequately protecting Plaintiff’s and Class Members’ Personal and
16 Medical Information;

17 c. Ensuring the confidentiality and integrity of electronic protected health
18 information it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. §
19 164.306(a)(1);

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

24
25
26 _____
27 ⁴ Breach Notification Rule, U.S. Dep’t of Health & Human Services,
28 <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis
added) (last visited Mar. 5, 2020).

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

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

6 g. Protecting against any reasonably anticipated threats or hazards to the
7 security or integrity of electronic protected health information in violation of 45 C.F.R. §
8 164.306(a)(2);

9 h. Protecting against reasonably anticipated uses or disclosures of
10 electronic protected health information that are not permitted under the privacy rules
11 regarding individually identifiable health information in violation of 45 C.F.R. §
12 164.306(a)(3);

13 i. Ensuring compliance with the HIPAA security standard rules by its
14 workforce in violation of 45 C.F.R. § 164.306(a)(4); and/or

15 j. Training all members of its workforce effectively on the policies and
16 procedures with respect to protected health information as necessary and appropriate for
17 the members of its workforce to carry out their functions and to maintain security of
18 protected health information, in violation of 45 C.F.R. § 164.530(b).

19 45. Defendant was also prohibited by the Federal Trade Commission Act (“FTC
20 Act”) (15 U.S.C. §45) from engaging in “unfair or deceptive acts or practices in or affecting
21 commerce.” The Federal Trade Commission (“FTC”) has concluded that a company’s
22 failure to maintain reasonable and appropriate data security for consumers’ sensitive personal
23 information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham*
24 *Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

25 46. As described before, Defendant is also required (by the CCRA, CMIA and
26 various other states’ laws and regulations) to protect Plaintiff’s and Class Members’ Personal
27 and Medical Information, and further, to handle any breach of the same in accordance with
28 applicable breach notification statutes.

1 47. In addition to its obligations under federal and state laws, Defendant owed a
2 duty to Affected Patients whose Personal and Medical Information was entrusted to
3 Defendant to exercise reasonable care in obtaining, retaining, securing, safeguarding,
4 deleting, and protecting the Personal and Medical Information in its possession from being
5 compromised, lost, stolen, accessed, and/or misused by unauthorized persons. Defendant
6 owed a duty to Affected Patients to provide reasonable security, including consistency with
7 industry standards and requirements, and to ensure that its computer systems and networks,
8 and the personnel responsible for them, adequately protected the Personal and Medical
9 Information of the Affected Patients.

10 48. Defendant owed a duty to Affected Patients whose Personal and Medical
11 Information was entrusted to Defendant to design, maintain, and test its computer systems
12 to ensure that the Personal and Medical Information in Defendant's possession was
13 adequately secured and protected.

14 49. Defendant owed a duty to Affected Patients whose Personal and Medical
15 Information was entrusted to Defendant to create and implement reasonable data security
16 practices and procedures to protect the Personal and Medical Information in its possession,
17 including adequately training its employees and others who accessed Personal and Medical
18 Information within its computer systems on how to adequately protect Personal and Medical
19 Information.

20 50. Defendant owed a duty to Affected Patients whose Personal and Medical
21 Information was entrusted to Defendant to implement processes that would detect a breach
22 on its data security systems in a timely manner.

23 51. Defendant owed a duty to Affected Patients whose Personal and Medical
24 Information was entrusted to Defendant to act upon data security warnings and alerts in a
25 timely fashion.

26 52. Defendant owed a duty to Affected Patients whose Personal and Medical
27 Information was entrusted to Defendant to adequately train and supervise its employees to
28 detect a breach on its data security systems in a timely manner.

1 53. Defendant owed a duty to Affected Patients whose Personal and Medical
2 Information was entrusted to Defendant to disclose if its computer systems and data security
3 practices were inadequate to safeguard individuals' Personal and Medical Information from
4 exfiltration because such an inadequacy would be a material fact in the decision to entrust
5 Personal and Medical Information with Defendant.

6 54. Defendant owed a duty to Affected Patients whose Personal and Medical
7 Information was entrusted to Defendant to disclose in a timely and accurate manner when
8 data breaches occurred.

9 55. Defendant owed a duty of care to Affected Patients because they were
10 foreseeable and probable victims of any inadequate data security practices.

11 **Defendant Was on Notice of Data Breach Threats and the Inadequacy of Its Data**
12 **Security**

13 56. Defendant was on notice that companies in the healthcare industry were targets
14 for cyberattacks.

15 57. Defendant was on notice that the FBI has been concerned about data security
16 in the healthcare industry. In August 2014, after a cyberattack on Community Health
17 Systems, Inc., the FBI warned companies within the healthcare industry that hackers were
18 targeting them. The warning stated that “[t]he FBI has observed malicious actors targeting
19 healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare
20 Information (PHI) and/or Personally Identifiable Information (PII).”⁵

21 58. The American Medical Association (“AMA”) has also warned healthcare
22 companies about the importance of protecting their patients’ confidential information:

23 Cybersecurity is not just a technical issue; it’s a patient safety issue.

24 AMA research has revealed that 83% of physicians work in a
25

26 _____
27 ⁵ Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014),
28 [http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-](http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820)
[idUSKBN0GK24U20140820](http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820) (last visited Mar. 5, 2020).

1 practice that has experienced some kind of cyberattack.
2 Unfortunately, practices are learning that cyberattacks not only
3 threaten the privacy and security of patients' health and financial
4 information, but also patient access to care.⁶

5 59. As implied by the above quote from the AMA, stolen Personal and Medical
6 Information can be used to interrupt important medical services themselves. This is an
7 imminent and certainly impending risk for all Affected Patients.

8 60. Defendant was on notice that the federal government has been concerned
9 about healthcare company data encryption. Defendant knew it kept protected health
10 information in its computer systems and yet did not encrypt its computer systems.

11 61. The United States Department of Health and Human Services' Office for Civil
12 Rights urges the use of encryption of data containing sensitive personal information. As long
13 ago as 2014, the Department fined two healthcare companies approximately two million
14 dollars for failing to encrypt laptops containing sensitive personal information. In
15 announcing the fines, Susan McAndrew, the DHHS's Office of Human Rights' deputy
16 director of health information privacy, stated "[o]ur message to these organizations is simple:
17 encryption is your best defense against these incidents."⁷

18 62. As a covered entity or business associate under HIPAA, Defendant should
19 have known about its weakness toward data security threats and sought better protection for
20 the Personal and Medical Information in its computer systems.

23 ⁶ Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med.
24 Ass'n (Oct. 4, 2019), [https://www.ama-assn.org/practice-](https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals)
25 [management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals](https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals)
(last visited Mar. 5, 2020).

26 ⁷ *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Dep't of Health and Human
27 Services (Apr. 22, 2014), available at [https://wayback.archive-](https://wayback.archive-it.org/3926/20150618190135/http://www.hhs.gov/news/press/2014pres/04/20140422b.html)
28 [it.org/3926/20150618190135/http://www.hhs.gov/news/press/2014pres/04/20140422b](https://wayback.archive-it.org/3926/20150618190135/http://www.hhs.gov/news/press/2014pres/04/20140422b.html)
html (last visited Mar. 5, 2020).

1 **It is Well Established That Data Breaches Lead to Identity Theft and Other Harms**

2 63. Plaintiff and Class Members have been injured by the disclosure and
3 exfiltration of their Personal and Medical Information in the Data Breach.

4 64. Each year, identity theft causes tens of billions of dollars of losses to victims in
5 the United States.⁸ Cyber criminals can leverage Plaintiff's and Class Members' Personal and
6 Medical Information that was exfiltrated in the Data Breach to commit thousands of crimes,
7 including opening new financial accounts in Affected Patients' names, taking out loans in
8 Affected Patients' names, using Affected Patients' names to obtain medical services, using
9 Affected Patients' Personal Information to file fraudulent tax returns, using Affected
10 Patients' health insurance information to rack up medical debts in their names, using
11 Affected Patients' health information to target them in other phishing and hacking intrusions
12 based on their individual health needs, using Affected Patients' information to obtain
13 government benefits, obtaining driver's licenses in Affected Patients' names but with another
14 person's photograph, and giving false information to police during an arrest. Even worse,
15 Affected Patients could be arrested for crimes identity thieves have committed.

16 65. Personal and Medical Information is such a valuable commodity to identity
17 thieves that once the information has been compromised, criminals often trade the
18 information on the cyber black-market for years.

19 66. This is not just speculative. As the FTC has reported, if hackers get access to
20 Personal and Medical Information, they *will* use it.⁹

21 67. For instance, with a stolen social security number, which is part of the Personal
22 and Medical Information compromised in the Data Breach, someone can open financial

23 _____
24 ⁸ *Facts + Statistics: Identity Theft and Cybercrime*, Insurance Info. Inst.,
25 <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (discussing
26 Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of
Complexity") (last visited Mar. 5, 2020).

27 ⁹ Ari Lazarus, *How fast will identity thieves use stolen info?*, Fed. Trade Comm'n (May 24, 2017),
28 [https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-
info](https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info) (last visited Mar. 5, 2020).

1 accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.¹⁰
2 Identity thieves can also use the information stolen from Breach Victims to qualify for
3 expensive medical care and leave them and their contracted health insurers on the hook for
4 massive medical bills.

5 68. Medical identity theft is one of the most common, most expensive, and most
6 difficult to prevent forms of identity theft. According to Kaiser Health News, “medical-
7 related identity theft accounted for 43 percent of all identity thefts reported in the United
8 States in 2013,” which is more “than identity thefts involving banking and finance, the
9 government and the military, or education.”¹¹

10 69. “Medical identity theft is a growing and dangerous crime that leaves its victims
11 with little to no recourse for recovery,” reported Pam Dixon, executive director of World
12 Privacy Forum. “Victims often experience financial repercussions and worse yet, they
13 frequently discover erroneous information has been added to their personal medical files due
14 to the thief’s activities.”¹²

15 70. As indicated by Jim Trainor, second in command at the FBI’s cyber security
16 division: “Medical records are a gold mine for criminals – they can access a patient’s name,
17 DOB, Social Security and insurance numbers, and even financial information all in one place.
18 Credit cards can be, say, five dollars or more where PHI can go from \$20 say up to – we’ve
19 seen \$60 or \$70 [(referring to prices on dark web marketplaces)].”¹³ A complete identity theft
20

21 ¹⁰ See, e.g., Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*,
22 Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/> (last visited Mar. 5, 2020).

23 ¹¹ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health
24 News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/> (last visited Mar. 5,
25 2020).

26 ¹² *Id.*

27 ¹³ IDEXperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data*, New
28 Ponemon Study Shows, <https://www.idexperts.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat> (last visited Mar. 5, 2020).

1 kit that includes health insurance credentials may be worth up to \$1,000 on the black
2 market.¹⁴

3 71. If, moreover, cyber criminals also manage to acquire financial information,
4 credit and debit cards, health insurance information, driver's licenses and passports, there is
5 no limit to the amount of fraud to which Defendant has exposed the Affected Patients.

6 72. The United States Government Accountability Office noted in a June 2007
7 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as
8 Social Security Numbers to open financial accounts, receive government benefits and incur
9 charges and credit in a person's name.¹⁵ As the GAO Report states, this type of identity theft
10 is the most harmful because it often takes some time for the victim to become aware of the
11 theft, and the theft can impact the victim's credit rating adversely.

12 73. In addition, the GAO Report states that victims of identity theft will face
13 "substantial costs and inconveniences repairing damage to their credit records" and their
14 "good name."¹⁶

15 74. Identity theft victims are frequently required to spend many hours and large
16 amounts of money repairing the impact to their credit. Identity thieves use stolen personal
17 information for a variety of crimes, including credit card fraud, phone or utilities fraud, and
18 bank/finance fraud.

21 _____
22 ¹⁴*Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings
23 from The Global State of Information Security Survey 2015,
24 [https://www.pwc.com/gx/en/consulting-services/information-security-
survey/assets/the-global-state-of-information-security-survey-2015.pdf](https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf) (last visited Mar. 5,
2020).

25 ¹⁵ *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is*
26 *Limited; However, the Full Extent Is Unknown* (June 2007), United States Government
27 Accountability Office, *available at* <https://www.gao.gov/new.items/d07737.pdf> (last visited
28 Mar. 5, 2020).

¹⁶ *Id.* at 2, 9.

1 75. There may be a time lag between when sensitive personal information is stolen
2 and when it is used. According to the GAO Report:

3 [L]aw enforcement officials told us that in some cases, *stolen data*
4 *may be held for up to a year or more before being used to*
5 *commit identity theft*. Further, once stolen data have been sold
6 or posted on the Web, *fraudulent use of that information may*
7 *continue for years*. As a result, studies that attempt to measure the
8 harm resulting from data breaches cannot necessarily rule out all
9 future harm.¹⁷

10 76. With access to an individual’s Personal and Medical Information, criminals can
11 do more than just empty a victim’s bank account – they can also commit all manner of fraud,
12 including: obtaining a driver’s license or official identification card in the victim’s name but
13 with the thief’s picture; using the victim’s name and SSN to obtain government benefits; or,
14 filing a fraudulent tax return using the victim’s information. In addition, identity thieves may
15 obtain a job using the victim’s SSN, rent a house, or receive medical services in the victim’s
16 name, and may even give the victim’s personal information to police during an arrest,
17 resulting in an arrest warrant being issued in the victim’s name.¹⁸

18 77. Personal and Medical Information is such a valuable commodity to identity
19 thieves that once the information has been compromised, criminals often trade the
20 information on the “cyber black-market” for years. As a result of recent large-scale data
21 breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers,
22 SSNs, and other Personal and Medical Information directly on various Internet websites
23 making the information publicly available.

24
25
26 ¹⁷ *Id.* at 29 (emphasis added).

27 ¹⁸ See Federal Trade Commission, *Warning Signs of Identity Theft*, available at
28 <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last visited Mar. 5, 2020).

1 78. A study by Experian found that the “average total cost” of medical identity
2 theft is “about \$20,000” per incident, and that a majority of victims of medical identity theft
3 were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore
4 coverage.¹⁹ Indeed, data breaches and identity theft have a crippling effect on individuals
5 and detrimentally impact the entire economy as a whole.

6 79. Medical databases are especially valuable to identity thieves. According to a
7 2012 Nationwide Insurance report, “[a] stolen medical identity has a \$50 street value –
8 whereas a stolen social security number, on the other hand, only sells for \$1.”²⁰ In fact, the
9 medical industry has experienced disproportionately higher instances of computer theft than
10 any other industry.

11 80. Furthermore, identity theft victims must spend countless hours and large
12 amounts of money repairing the impact to their credit.²¹

13 81. To date, other than providing 24 months of credit monitoring, Defendant does
14 not appear to be taking any measures to assist Plaintiff and Class Members other than telling
15 them to simply do the following:

- 16 • “remain vigilant”;
- 17 • “review [] account statements and monitor [] credit reports”;
- 18 • “report suspected incidents of identity theft to local law enforcement or
19 to the Attorney General”;
- 20 • obtain a copy of free credit reports;

21
22 ¹⁹ See Elinor Mills, Study: Medical identity theft is costly for victims, CNET (Mar. 3, 2010),
23 <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last
24 visited Mar. 5, 2020).

25 ²⁰ Study: Few Aware of Medical Identity Theft Risk, Claims Journal,
26 <https://www.claimsjournal.com/news/national/2012/06/14/208510.htm> (last visited
Mar. 5, 2020).

27 ²¹ “Guide for Assisting Identity Theft Victims,” Federal Trade Commission, 4 (Sept. 2013),
28 <https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf> (last
visited Mar. 5, 2020).

- 1 • contact the FTC, the state Attorney General’s office, and/or local law
- 2 enforcement;
- 3 • enact a security freeze on credit files; and
- 4 • create a fraud alert.

5 None of these recommendations, however, require Defendant to expend any effort to
6 protect Plaintiff’s and Class Members’ Personal and Medical Information.

7 82. Defendant’s failure to adequately protect Plaintiff’s and Class Members’
8 Personal and Medical Information has resulted in Plaintiff and Class Members having to
9 undertake these tasks, which require extensive amounts of time, calls, and, for many of the
10 credit and fraud protection services, payment of money – while Defendant sits by and does
11 nothing to assist those affected by the incident. Instead, as Defendant’s notice indicates, it is
12 putting the burden on the Plaintiff and Class Members to discover possible fraudulent
13 activity and identity theft.

14 83. Defendant’s offer of 24 months of identity monitoring to Plaintiff and Class
15 Members is woefully inadequate. While some harm has begun already, the worst may be yet
16 to come. There may be a time lag between when harm occurs versus when it is discovered,
17 and also between when Personal and Medical Information is acquired and when it is used.
18 Furthermore, identity monitoring only alerts someone to the fact that they have already been
19 the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person’s Personal
20 and Medical Information) – it does not prevent identity theft.²² This is especially true for
21 many kinds of medical identity theft, for which most credit monitoring plans provide little
22 or no monitoring or protection.

23 84. As a direct and proximate result of the Data Breach, Plaintiff and Class
24 Members have been placed at an imminent, immediate, and continuing increased risk of
25

26
27 ²² See, e.g., Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017,
28 <https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html> (last visited Mar. 5, 2020).

1 harm from fraud and identity theft. Plaintiff and Class Members must now take the time
2 and effort to mitigate the actual and potential impact of the Data Breach on their everyday
3 lives, including placing “freezes” and “alerts” with credit reporting agencies, contacting their
4 financial institutions, healthcare providers, closing or modifying financial accounts, and
5 closely reviewing and monitoring bank accounts, credit reports, and health insurance account
6 information for unauthorized activity for years to come.

7 85. Plaintiff and the Class Members have suffered, continue to suffer and/or will
8 suffer, actual harms for which they are entitled to compensation, including:

- 9 a. Trespass, damage to, and theft of their personal property including
10 Personal and Medical Information;
- 11 b. Improper disclosure of their Personal and Medical Information;
- 12 c. The imminent and certainly impending injury flowing from potential
13 fraud and identity theft posed by their Personal and Medical Information being
14 placed in the hands of criminals;
- 15 d. The imminent and certainly impending risk of having their confidential
16 medical information used against them by spam callers to defraud them;
- 17 e. Damages flowing from Defendant untimely and inadequate notification
18 of the data breach;
- 19 f. Loss of privacy suffered as a result of the Data Breach;
- 20 g. Ascertainable losses in the form of out-of-pocket expenses and the value
21 of their time reasonably expended to remedy or mitigate the effects of the data
22 breach;
- 23 h. Ascertainable losses in the form of deprivation of the value of Affected
24 Patients’ personal information for which there is a well-established and
25 quantifiable national and international market;
- 26 i. The loss of use of and access to their credit, accounts, and/or funds;
- 27 j. Damage to their credit due to fraudulent use of their Personal and
28 Medical Information; and

1 k. Increased cost of borrowing, insurance, deposits and other items which
2 are adversely affected by a reduced credit score.

3 86. Moreover, Plaintiff and Class Members have an interest in ensuring that their
4 information, which remains in the possession of Defendant, is protected from further
5 breaches by the implementation of security measures and safeguards.

6 87. Defendant itself acknowledged the harm caused by the Data Breach because it
7 offered Plaintiff and Class Members 24 months of identity theft monitoring services. 24
8 months of identity theft monitoring is woefully inadequate to protect Plaintiff and Class
9 Members from a lifetime of identity theft risk and does nothing to reimburse Plaintiff and
10 Class Members for the injuries they have already suffered.

11 **CHOICE OF LAW**

12 88. The State of California has a significant interest in regulating the conduct of
13 businesses operating within its borders. California seeks to protect the rights and interests of
14 all California residents and citizens of the United States against a company headquartered
15 and doing business in California. California has a greater interest in the nationwide claims of
16 Plaintiff and members of the Nationwide Class than any other state and is most intimately
17 concerned with the claims and outcome of this litigation.

18 89. The corporate headquarters of Defendant, located in San Juan Capistrano,
19 California, is the “nerve center” of its business activities – the place where its officers direct,
20 control, and coordinate the company’s activities, including its data security functions and
21 policy, financial, and legal decisions.

22 90. Defendant’s response to the Data Breach at issue here, and corporate decisions
23 surrounding such response, were made from and in California.

24 91. Defendant’s breaches of duty to Plaintiff and Nationwide Class members
25 emanated from California.

26 92. Application of California law to the Nationwide Class with respect to Plaintiff’s
27 and Class Members’ claims is neither arbitrary nor fundamentally unfair because California
28

1 has significant contacts and a significant aggregation of contacts that create a state interest
2 in the claims of Plaintiff and the Nationwide Class.

3 93. Under California's choice of law principles, which are applicable to this action,
4 the common law of California applies to the nationwide common law claims of all
5 Nationwide Class members. Additionally, given California's significant interest in regulating
6 the conduct of businesses operating within its borders, California's Unfair Competition Law
7 and Confidentiality of Medical Information Act may be applied to non-resident plaintiffs as
8 against this resident defendant.

9 **CLASS ALLEGATIONS**

10 94. Plaintiff brings this class action lawsuit individually and on behalf of the
11 proposed Class Members under Rule 23 of the Federal Rules of Civil Procedure.

12 95. Plaintiff seeks certification of a Nationwide Class, a California Sub-Class, and
13 a Pennsylvania Sub-Class defined as follows:

14 Nationwide Class: All persons in the United States whose Personal
15 and Medical Information was compromised as a result of the
16 Sunshine Data Breach announced by Sunshine on or around
17 January 21, 2020.

18 96. In the alternative to the Nationwide Class, Plaintiff seeks
19 certification of the following California state class:

20 California Sub-Class: All persons in the State of California whose
21 Personal and Medical Information was compromised as a result of
22 the Sunshine Data Breach announced by Sunshine on or around
23 January 21, 2020.

24 97. In the alternative to the Nationwide Class, Plaintiff seeks
25 certification of the following Pennsylvania state class:

26 Pennsylvania Sub-Class: All persons in the State of Pennsylvania
27 whose Personal and Medical Information was compromised as a
28

1 result of the Sunshine Data Breach announced by Sunshine on or
2 around January 21, 2020.

3 98. Specifically excluded from the Classes are Defendant and any entities in which
4 Defendant has a controlling interest, Defendant's agents and employees, the judge to whom
5 this action is assigned, members of the judge's staff, and the judge's immediate family.

6 99. **Numerosity:** Plaintiff does not know the exact number of Class Members, but
7 believes the Classes comprise approximately 3,500 individuals throughout the United States.
8 As such, Class Members are so numerous that joinder of all members is impracticable.

9 100. **Commonality:** Common questions of law and fact exist and predominate over
10 any questions affecting only individual Class Members. The common questions include:

- 11 a. Whether Defendant engaged in the conduct alleged herein;
- 12 b. Whether Defendant failed to adequately safeguard Plaintiff's and Class
13 Members' Personal and Medical Information;
- 14 c. Whether Defendant failed to protect Plaintiff's and Class Members'
15 Personal and Medical Information properly and/or as promised;
- 16 d. Whether Defendant's computer system and data security practices used
17 to protect Plaintiff's and the Class Members' Personal and Medical Information violated
18 federal, state or local laws, or Defendant's duties;
- 19 e. Whether Defendant engaged in unfair, unlawful, or deceptive practices
20 by failing to safeguard Plaintiff's and Class Members' Personal and Medical Information;
- 21 f. Whether Defendant violated the consumer protection statutes, data
22 breach notification statutes, state unfair insurance practice statutes, state insurance privacy
23 statutes, and/or state medical privacy statutes applicable to Plaintiff and Class Members;
- 24 g. Whether Defendant failed to notify Plaintiff and Class Members about
25 the Data Breach as soon as practical and without delay after the Data Breach was discovered;
- 26 h. Whether Defendant acted negligently in failing to safeguard Plaintiff's
27 and Class Members' Personal and Medical Information;

1 i. Whether Defendant express or implied contractual obligations to
2 protect the confidentiality of Plaintiff's and the Class Members' Personal and Medical
3 Information, and to have reasonable data security measures;

4 j. Whether Defendant's conduct described herein constitutes a breach of
5 contract with Plaintiff and Class Members;

6 k. Whether Plaintiff and Class Members are entitled to damages as a result
7 of Defendant's wrongful conduct;

8 l. Whether Plaintiff and Class Members are entitled to restitution as a
9 result of Defendant's wrongful conduct;

10 m. What equitable relief is appropriate to redress Defendant's wrongful
11 conduct; and

12 n. What injunctive relief is appropriate to redress the imminent and
13 currently ongoing harm faced by Plaintiff and Class Members.

14 101. **Typicality:** Plaintiff's claims are typical of the claims of the Class Members.
15 Plaintiff and Class Members were injured through Defendant's uniform misconduct and
16 their legal claims arise from the same core practices of Defendant.

17 102. **Adequacy:** Plaintiff will fairly and adequately represent and protect the
18 interests of the Classes and has retained counsel competent and experienced in complex
19 litigation and class actions. Plaintiff has no interests antagonistic to those of the Classes, and
20 there are no defenses unique to Plaintiff. Plaintiff and his counsel are committed to
21 prosecuting this action vigorously on behalf of the members of the proposed Classes and
22 have the financial resources to do so. Neither Plaintiff nor his counsel have any interest
23 adverse to those of the other members of the Classes.

24 103. **Risks:** The proposed action meets the requirements of Fed. R. Civ. P. 23
25 because prosecution of separate actions by individual members of the Classes would create
26 a risk of inconsistent or varying adjudications that would establish incompatible standards
27 for Defendant or would be dispositive of the interests of members of the proposed Classes.
28

1 Furthermore, Sunshine’s database still exists, and is still vulnerable to future attacks – one
2 standard of conduct is needed to ensure the future safety of Sunshine’s database.

3 104. **Injunctive Relief:** The proposed action meets the requirements of Fed. R. Civ.
4 P. 23(b)(2) because Defendant has acted or has refused to act on grounds generally
5 applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is
6 appropriate as to the Classes as a whole.

7 105. **Predominance:** The proposed action meets the requirements of Fed. R. Civ.
8 P. 23(b)(3) because questions of law and fact common to the Classes predominate over any
9 questions that may affect only individual Class Members in the proposed Classes.

10 106. **Superiority:** The proposed action also meets the requirements of Fed. R. Civ.
11 P. 23(b)(3) because a class action is superior to all other available methods of fairly and
12 efficiently adjudicating this dispute. The injury sustained by each Class Member, while
13 meaningful on an individual basis, is not of such magnitude that it is economically feasible
14 to prosecute individual actions against Defendant. Even if it were economically feasible,
15 requiring more than 3,500 injured plaintiffs to file individual suits would impose a crushing
16 burden on the court system and almost certainly lead to inconsistent judgments. By contrast,
17 class treatment will present far fewer management difficulties and provide the benefits of a
18 single adjudication, economies of scale, and comprehensive supervision by a single court.
19 Plaintiff anticipates no unusual difficulties in managing this class action.

20 107. **Certification of Particular Issues:** In the alternative, this action may be
21 maintained as class action with respect to particular issues in accordance with Fed. R. Civ. P.
22 23(c)(4).

23 108. Finally, all members of the purposed Classes are readily ascertainable.
24 Defendant has access to addresses and other contact information for members of the
25 Classes, which can be used to identify Class Members.

1 **COUNT I**

2 **NEGLIGENCE**

3 109. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

4 110. This count is brought on behalf of all Classes.

5 111. Defendant collected and stored the Personal and Medical Information of
6 Plaintiff and Class Members.

7 112. Defendant knew, or should have known, of the risks inherent in collecting and
8 storing the Personal and Medical Information of Plaintiff and Class Members.

9 113. Defendant owed duties of care to Plaintiff and Class Members whose Personal
10 and Medical Information had been entrusted with Defendant.

11 114. Defendant breached its duties to Plaintiff and Class Members by failing to
12 provide fair, reasonable, or adequate computer systems and data security practices to
13 safeguard Plaintiff's and Class Members' Personal and Medical Information.

14 115. Defendant acted with wanton disregard for the security of Plaintiff's and Class
15 Members' Personal and Medical Information. Defendant knew or should have known that
16 it had inadequate computer systems and data security practices to safeguard such
17 information, and Defendant knew or should have known that hackers were attempting to
18 access the Personal and Medical Information in health care databases, such as theirs.

19 116. A "special relationship" exists between Defendant and the Plaintiff and Class
20 Members. Defendant entered into a "special relationship" with Plaintiff and Class Members
21 by placing their Personal and Medical Information in the Sunshine Database – information
22 that Plaintiff and Class Members had been required to provide to Defendant.

23 117. But for Defendant's wrongful and negligent breach of its duties owed to
24 Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

25 118. The injury and harm suffered by Plaintiff and Class Members was the
26 reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should
27 have known that it was failing to meet its duties, and that Defendant's breach would cause
28

1 Plaintiff and Class Members to experience the foreseeable harms associated with the
2 exposure of their Personal and Medical Information.

3 119. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and
4 Class Members now face an increased risk of future harm.

5 120. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and
6 Class Members have suffered injury and are entitled to damages in an amount to be proven
7 at trial.

8 **COUNT II**

9 **NEGLIGENCE PER SE**

10 121. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

11 122. This count is brought on behalf of all Classes.

12 123. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant
13 had a duty to provide fair and adequate computer systems and data security practices to
14 safeguard Plaintiff's and Class Members' Personal and Medical Information.

15 124. Pursuant to HIPAA (42 U.S.C. § 1302d *et. seq.*), Defendant had a duty to
16 implement reasonable safeguards to protect Plaintiff's and Class Members' Personal and
17 Medical Information.

18 125. Pursuant to Cal. Civ. Code § 56 *et seq.*, Defendant had a duty to implement and
19 maintain reasonable security procedures and practices to safeguard Plaintiff's and Class
20 Members' Personal and Medical Information.

21 126. Defendant breached its duties to Plaintiff and Class Members under the Federal
22 Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d *et. seq.*), and Cal. Civ.
23 Code § 56 *et seq.* by failing to provide fair, reasonable, or adequate computer systems and
24 data security practices to safeguard Plaintiff's and Class Members' Personal and Medical
25 Information.

26 127. Defendant's failure to comply with applicable laws and regulations constitutes
27 negligence *per se*.

1 128. But for Defendant's wrongful and negligent breach of its duties owed to
2 Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

3 129. The injury and harm suffered by Plaintiff and Class Members was the
4 reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should
5 have known that it was failing to meet its duties, and that Defendant's breach would cause
6 Plaintiff and Class Members to experience the foreseeable harms associated with the
7 exposure of their Personal and Medical Information.

8 130. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and
9 Class Members now face an increased risk of future harm.

10 131. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and
11 Class Members have suffered injury and are entitled to damages in an amount to be proven
12 at trial.

13 **COUNT III**

14 **BREACH OF CONTRACT**

15 132. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

16 133. This count is brought on behalf of all Classes.

17 134. As the operator of drug and alcohol rehabilitation facilities, Defendant entered
18 into contracts with Plaintiff and Class Members.

19 135. The promises and representations described above relating to HIPAA, CMIA,
20 and industry practices, and about Defendant's purported concern about its patients' privacy
21 rights became terms of the contract between it and its customers, including Plaintiff and
22 Class Members.

23 136. Defendant breached these promises by failing to comply with HIPAA, CMIA,
24 and reasonable industry practices.

25 137. As a result of Defendant's breach of these terms, Plaintiff and Class Members
26 have been harmed and put at risk of future harm.

1 138. Plaintiff and Class Members are therefore entitled to damages, including
2 restitution and unjust enrichment, declaratory and injunctive relief, and attorney fees, costs,
3 and expenses.

4 **COUNT IV**

5 **BREACH OF IMPLIED CONTRACT**

6 139. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

7 140. This count is brought on behalf of all Classes.

8 141. When Plaintiff and the Class Members provided their Personal and Medical
9 Information to Defendant when seeking treatment, they entered into implied contracts in
10 which Defendant agreed to comply with its statutory and common law duties to protect their
11 Personal and Medical Information and to timely notify them in the event of a data breach.

12 142. Defendant required its patients (including Plaintiff and Class Members) to
13 provide Personal and Medical Information in order to receive treatment from Defendant.

14 143. Defendant affirmatively represented that it collected and stored the Personal
15 and Medical Information of Plaintiff and Class Members in compliance with HIPAA, the
16 CMIA, and other statutory and common law duties, and using reasonable, industry standard
17 means.

18 144. Based on the implicit understanding and on Defendant's representations (as
19 described above), Plaintiff and Class Members accepted Defendant's offers and provided
20 Defendant with their Personal and Medical Information.

21 145. Plaintiff and Class Members would not have provided their Personal and
22 Medical Information to Defendant had they known that Defendant would not safeguard
23 their Personal and Medical Information as promised or provide timely notice of a data
24 breach.

25 146. Plaintiff and Class Members fully performed their obligations under the implied
26 contracts with Defendant.

1 147. Defendant breached the implied contracts by failing to safeguard Plaintiff's and
2 Class Members' personal information and failing to provide them with timely and accurate
3 notice of the Data Breach.

4 148. The losses and damages Plaintiff and Class Members sustained (as described
5 above) were the direct and proximate result of Defendant's breach of the implied contract
6 with Plaintiff and Class Members.

7 **COUNT V**

8 **BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR**

9 **DEALING**

10 149. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

11 150. This count is brought on behalf of all Classes.

12 151. As described above, Defendant made promises and representations to Plaintiff
13 and Class Members that it would comply with HIPAA, the CMIA and other applicable laws
14 and industry best practices.

15 152. These promises and representations became a part of the contract between
16 Defendant and Plaintiff and Class Members.

17 153. While Defendant had discretion in the specifics of how it met the applicable
18 laws and industry standards, this discretion was governed by an implied covenant of good
19 faith and fair dealing.

20 154. Defendant breached this implied covenant when it engaged in acts and/or
21 omissions that are declared unfair trade practices by the FTC and state statutes and
22 regulations (including California's UCL), and when it engaged in unlawful practices under
23 HIPAA, the CMIA, and other laws. These acts and omissions included: representing that it
24 would maintain adequate data privacy and security practices and procedures to safeguard the
25 Personal and Medical Information from unauthorized disclosures, releases, data breaches,
26 and theft; omitting, suppressing, and concealing the material fact of the inadequacy of the
27 privacy and security protections for Plaintiff's and Class Members' Personal and Medical
28 Information; and failing to disclose to Plaintiff and Class Members at the time they provided

1 their Personal and Medical Information to it that Defendant's data security systems,
2 including training, auditing, and testing of employees, failed to meet applicable legal and
3 industry standards.

4 155. Plaintiff and Class Members did all or substantially all the significant things that
5 the contract required them to do.

6 156. Likewise, all conditions required for Defendant's performance were met.

7 157. Defendant's acts and omissions unfairly interfered with Plaintiff's and Class
8 Members' rights to receive the full benefit of their contracts.

9 158. Plaintiff and Class Members have been harmed by Defendant's breach of this
10 implied covenant in the many ways described above, including overpayment for products
11 and services, actual identity theft and/or imminent risk of certainly impending and
12 devastating identity theft that exists now that cyber criminals have their Personal and Medical
13 Information, and the attendant long-term expense of attempting to mitigate and insure
14 against these risks.

15 159. Defendant is liable for this breach of these implied covenants whether or not
16 it is found to have breached any specific express contractual term.

17 160. Plaintiff and Class Members are entitled to damages, including compensatory
18 damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and
19 expenses.

20 **COUNT VI**

21 **UNJUST ENRICHMENT**

22 161. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

23 162. This count is brought on behalf of all Classes.

24 163. Plaintiff and Class Members conferred a monetary benefit on Defendant.
25 Defendant received and retained money belonging to Plaintiff and Class Members either
26 directly through copayments and coinsurance or indirectly through health insurance/medical
27 plans they had paid for.

1 164. Defendant had knowledge of the benefits conferred on it by Plaintiff and the
2 Class Members.

3 165. The money that Plaintiff and Class Members paid to Defendant was supposed
4 to be used by Defendant, in part, to pay for the costs of HIPAA and CMIA compliance and
5 reasonable data privacy and security practices and procedures.

6 166. As a result of Defendant's conduct, Plaintiff and Class Members suffered
7 damages in an amount equal to the difference in value between health care services with the
8 reasonable data privacy and security practices and procedures that they paid for, and the
9 inadequate health care services without reasonable data privacy and security practices and
10 procedures that they received.

11 167. Under principals of equity and good conscience, Defendant should not be
12 permitted to retain the money belonging to Plaintiff and Class Members because Defendant
13 failed to implement (or to adequately implement) the data privacy and security practices and
14 procedures that Plaintiff and Class Members paid for and that were otherwise mandated by
15 HIPAA regulations, federal, state, and local laws, and industry standards.

16 168. Defendant should be compelled to disgorge into a common fund for the
17 benefit of Plaintiff and Class members all unlawful or inequitable proceeds that Defendant
18 received.

19 169. A constructive trust should be imposed on all unlawful or inequitable sums
20 received by Defendant traceable to Plaintiff and Class Members.

21 **COUNT VII**

22 **VIOLATIONS OF CALIFORNIA'S UNFAIR COMPETITION LAW**

23 **Cal. Bus. & Prof. Code §17200, et seq.**

24 170. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

25 171. This count is brought on behalf of all Classes or alternatively the California
26 Sub-Class.

27 172. Defendant is both organized under the laws of California and headquartered in
28 California. Defendant violated California's Unfair Competition Law ("UCL"), Cal. Bus. Prof.

1 Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices
2 and unfair, deceptive, untrue or misleading advertising that constitute acts of “unfair
3 competition” as defined in the UCL, including, but not limited to, the following:

4 a. by representing and advertising that it would maintain adequate data
5 privacy and security practices and procedures to safeguard Plaintiff’s and Class Members’
6 Personal and Medical Information from unauthorized disclosure, release, data breach, and
7 theft; representing and advertising that it did and would comply with the requirement of
8 relevant federal and state laws pertaining to the privacy and security of Plaintiff’s and Class
9 Members’ Personal and Medical Information; and omitting, suppressing, and concealing the
10 material fact of the inadequacy of the privacy and security protections for Plaintiff’s and
11 Class Members’ Personal and Medical Information;

12 b. by soliciting and collecting Plaintiff’s and Class Members’ Personal and
13 Medical Information with knowledge that the information would not be adequately
14 protected; and by storing Plaintiff’s and Class members’ Personal and Medical Information
15 in an unsecure electronic environment;

16 c. by failing to disclose the Data Breach in a timely and accurate manner,
17 in violation of Cal. Civ. Code §1798.82;

18 d. by violating the privacy and security requirements of HIPAA, 42 U.S.C.
19 §1302d, *et seq.*;

20 e. by violating the CMIA, Cal. Civ. Code § 56, *et seq.*; and

21 f. by violating the CCRA, Cal. Civ. Code § 1798.82.

22 173. These unfair acts and practices were immoral, unethical, oppressive,
23 unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class
24 Members. Defendant’s practice was also contrary to legislatively declared and public policies
25 that seek to protect consumer data and ensure that entities who solicit or are entrusted with
26 personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15
27 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq.*, CMIA, Cal. Civ. Code § 56, *et seq.*, and the
28 CCRA, Cal. Civ. Code § 1798.81.5.

1 174. As a direct and proximate result of Defendant’s unfair and unlawful practices
2 and acts, Plaintiff and Class Members were injured and lost money or property, including
3 but not limited to the overpayments Defendant received to take reasonable and adequate
4 security measures (but did not), the loss of their legally protected interest in the
5 confidentiality and privacy of their Personal and Medical Information, and additional losses
6 described above.

7 175. Defendant knew or should have known that its computer systems and data
8 security practices were inadequate to safeguard Plaintiff’s and Class Members’ Personal and
9 Medical Information and that the risk of a data breach or theft was highly likely. Defendant’s
10 actions in engaging in the above-named unfair practices and deceptive acts were negligent,
11 knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and
12 Class Members.

13 176. The conduct and practices described above emanated from California where
14 decisions related to Defendant’s advertising and data security were made.

15 177. Plaintiff seeks relief under the UCL, including restitution to Class Members of
16 money or property that the Defendant may have acquired by means of Defendant’s
17 deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and
18 expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

19 **COUNT VIII**

20 **VIOLATIONS OF CALIFORNIA’S CONSUMER RECORDS ACT**

21 **Cal. Civ. Code § 1798.82, et seq.**

22 178. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

23 179. This count is brought on behalf of all Classes or alternatively the California
24 Sub-Class.

25 180. Section 1798.2 of the California Civil Code requires any “person or business
26 that conducts business in California, and that owns or licenses computerized data that
27 includes personal information” to “disclose any breach of the security of the system
28 following discovery or notification of the breach in the security of the data to any resident

1 of California whose unencrypted personal information was, or is reasonably believed to have
2 been, acquired by an unauthorized person.” Under section 1798.82, the disclosure “shall be
3 made in the most expedient time possible and without unreasonable delay”

4 181. The CCRA further provides: “Any person or business that maintains
5 computerized data that includes personal information that the person or business does not
6 own shall notify the owner or licensee of the information of any breach of the security of
7 the data immediately following discovery, if the personal information was, or is reasonably
8 believed to have been, acquired by an unauthorized person.” Cal. Civ. Code § 1798.82(b).

9 182. Any person or business that is required to issue a security breach notification
10 under the CCRA shall meet all of the following requirements:

- 11 a. The security breach notification shall be written in plain language;
- 12 b. The security breach notification shall include, at a minimum, the
13 following information:
- 14 i. The name and contact information of the reporting person or
15 business subject to this section;
- 16 ii. A list of the types of personal information that were or are reasonably
17 believed to have been the subject of a breach;
- 18 iii. If the information is possible to determine at the time the notice is
19 provided, then any of the following:
- 20 1. The date of the breach;
- 21 2. The estimated date of the breach; or
- 22 3. The date range within which the breach occurred. The
23 notification shall also include the date of the notice.
- 24 iv. Whether notification was delayed as a result of a law enforcement
25 investigation, if that information is possible to determine at the time
26 the notice is provided;
- 27 v. A general description of the breach incident, if that information is
28 possible to determine at the time the notice is provided; and

1 vi. The toll-free telephone numbers and addresses of the major credit
2 reporting agencies if the breach exposed a Social Security number or
3 a driver's license or California identification card number.

4 183. The Data Breach described herein constituted a "breach of the security system"
5 of Defendant.

6 184. As alleged above, Defendant unreasonably delayed informing Plaintiff and
7 Class Members about the Data Breach, affecting their Personal and Medical Information,
8 after Defendant knew the Data Breach had occurred.

9 185. Defendant failed to disclose to Plaintiff and Class Members, without
10 unreasonable delay and in the most expedient time possible, the breach of security of their
11 unencrypted, or not properly and securely encrypted, Personal and Medical Information
12 when Defendant knew or reasonably believed such information had been compromised.

13 186. Defendant's ongoing business interests gave Defendant incentive to conceal
14 the Data Breach from the public to ensure continued revenue.

15 187. Upon information and belief, no law enforcement agency instructed Defendant
16 that timely notification to Plaintiff and the Class Members would impede its investigation.

17 188. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and
18 Class Members were deprived of prompt notice of the Data Breach and were thus prevented
19 from taking appropriate protective measures, such as securing identity theft protection or
20 requesting a credit freeze. These measures could have prevented some of the damages
21 suffered by Plaintiff and Class Members because their stolen information would have had
22 less value to identity thieves.

23 189. As a result of Defendant's violation of Cal. Civ. Code § 1798.82, Plaintiff and
24 Class Members suffered incrementally increased damages separate and distinct from those
25 simply caused by the Data Breach itself.

26 190. Plaintiff and Class Members seek all remedies available under Cal. Civ. Code §
27 1798.84, including, but not limited to the damages suffered by Plaintiff and the other Class
28 Members as alleged above and equitable relief.

1 191. Defendant’s misconduct as alleged herein is fraud under Cal. Civ. Code §
2 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendant
3 conducted with the intent on the part of Defendant of depriving Plaintiff and Class Members
4 of “legal rights or otherwise causing injury.” In addition, Defendant’s misconduct as alleged
5 herein is malice or oppression under Cal. Civ. Code § 3294(c)(1) and (c)(2) in that it was
6 despicable conduct carried on by Defendant with a willful and conscious disregard of the
7 rights or safety of Plaintiff and Class Members and despicable conduct that has subjected
8 Plaintiff and Class Members to hardship in conscious disregard of their rights. As a result,
9 Plaintiff and Class Members are entitled to punitive damages against Defendant under Cal.
10 Civ. Code § 3294(a).

11 **COUNT IX**

12 **VIOLATIONS OF CALIFORNIA’S CONFIDENTIALITY OF MEDICAL**
13 **INFORMATION ACT, Cal. Civ. Code § 56 et seq.**

14 192. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

15 193. This count is brought on behalf of all Classes or alternatively the California
16 Sub-Class.

17 194. Defendant is a “Contractor” as defined by Cal. Civ. Code § 56.05(d) and/or a
18 “Provider of Health Care” as expressed in Cal. Civ. Code § 56.06.

19 195. Plaintiff and Class Members are “Patients” as defined by Cal. Civ. Code §
20 56.05(k).

21 196. The Plaintiff’s and Class Members’ Personal and Medical Information that was
22 the subject of the Data Breach included “Medical Information” as defined by Cal. Civ. Code
23 § 56.05(j).

24 197. In violation of California’s Confidentiality of Medical Information Act
25 (“CMIA”), Defendant disclosed Medical Information of Plaintiff and Class Members
26 without first obtaining an authorization.

1 198. In violation of the CMIA, Defendant intentionally shared, sold, used for
2 marketing, or otherwise used Medical Information of Plaintiff and Class Members for a
3 purpose not necessary to provide health care services to Plaintiff or Class Members.

4 199. In violation of the CMIA, Defendant further disclosed Medical Information
5 regarding Plaintiff and Class Members to persons or entities not engaged in providing direct
6 health care services to Plaintiff or Class Members or their providers of health care or health
7 care service plans or insurers or self-insured employers.

8 200. In violation of the CMIA, Defendant created, maintained, preserved, stored,
9 abandoned, destroyed, or disposed of Medical Information of Plaintiff and Class Members
10 in a manner that did not preserve the confidentiality of the information contained therein.

11 201. In violation of the CMIA, Defendant negligently created, maintained,
12 preserved, stored, abandoned, destroyed, or disposed of Medical Information of Plaintiff
13 and Class Members.

14 202. In violation of the CMIA, Defendant's electronic health record systems or
15 electronic medical record systems did not protect and preserve the integrity of Plaintiff's and
16 Class Members' Medical Information.

17 203. In violation of the CMIA, Defendant negligently released confidential
18 information and records of Plaintiff and Class Members.

19 204. In violation of the CMIA, Defendant negligently disclosed Medical
20 Information of Plaintiff and Class Members.

21 205. In violation of the CMIA, Defendant knowingly and willfully obtained,
22 disclosed, and/or used Medical Information of Plaintiff and Class Members.

23 206. As a direct and proximate result of Defendant's violation of Cal. Civ. Code §
24 56 *et seq.*, Plaintiff and Class Members now face an increased risk of future harm.

25 207. As a direct and proximate result of Defendant's violation of Cal. Civ. Code §
26 56 *et seq.*, Plaintiff and Class Members have suffered injury and are entitled to damages in an
27 amount to be proven at trial.

1 **COUNT X**

2 **VIOLATIONS OF CALIFORNIA’S CONSUMER PRIVACY ACT**

3 **Cal. Civ. Code § 1798.100, et seq.**

4 208. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

5 209. This count is brought in the alternative to Plaintiff’s CMIA count.

6 210. This count is brought on behalf of all Classes or alternatively the California
7 Sub-Class.

8 211. Through the above-detailed conduct, Defendant violated California’s
9 Consumer Privacy Act (“CCPA”) by subjecting the nonencrypted and nonredacted Personal
10 and Medical Information of Plaintiff and Class members to unauthorized access and
11 exfiltration, theft, or disclosure as a result of Defendant’s violation of its duty to implement
12 and maintain reasonable security procedures and practices appropriate to the nature and
13 protection of that information. Cal. Civ. Code § 1798.150(a).

14 212. In accordance with Cal. Civ. Code § 1798.150(b), prior to the filing of this
15 Complaint, Plaintiff’s counsel served Defendant with notice of these CCPA violations by
16 certified mail, return receipt requested.

17 213. On behalf of Class members, Plaintiff seeks injunctive relief in the form of an
18 order enjoining Defendant from continuing to violate the CCPA. If Defendant fails to
19 respond to Plaintiff’s notice letter or agree to rectify the violations detailed above, Plaintiff
20 also will seek actual, punitive, and statutory damages, restitution, attorneys’ fees and costs,
21 and any other relief the Court deems proper as a result of Defendant’s CCPA violations.

22 **COUNT XI**

23 **VIOLATIONS OF PENNSYLVANIA’S UNFAIR TRADE PRACTICES ACT**

24 **73 Pa. Stat. Ann. § 201-1, et seq.**

25 214. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

26 215. This count is brought on behalf of the Pennsylvania Sub-Class.

27 216. Plaintiff, the alternative Pennsylvania Sub-Class, and Defendant are “persons”
28 within the meaning of 73 Pa. Cons. Stat. Ann. §201-2(2).

1 217. Plaintiff and the alternative Pennsylvania Sub-Class purchased Defendant's
2 products and services for personal, family, or household purposes within the meaning of 73
3 Pa. Cons. Stat. Ann. §201-9.2.

4 218. Plaintiff and the alternative Pennsylvania Sub-Class directly or indirectly
5 purchased products and services from Defendant in the course of trade or commerce within
6 the meaning of 73 Pa. Stat. Ann. §201-2(3).

7 219. Defendant engaged in unlawful, unfair, and deceptive acts and practices,
8 misrepresentations, and the concealment, suppression, and omission of material facts with
9 respect to the sale and advertisement of the products and services purchased by Plaintiff and
10 the alternative Pennsylvania Sub-Class in violation of 73 Pa. Stat. Ann. §201-2, including but
11 not limited to the following:

12 a. Defendant misrepresented material facts pertaining to the sale of
13 products and services to the alternative Pennsylvania Sub-Class by representing that it would
14 maintain adequate data privacy and security practices and procedures to safeguard the
15 Personal and Medical Information of the alternative Pennsylvania Sub-Class from
16 unauthorized disclosure, release, data breach, and theft in violation of 73 Pa. Stat. Ann. §
17 201-2(4)(v), (ix), and (xxi);

18 b. Defendant misrepresented material facts pertaining to the sale of
19 products and services to the alternative Pennsylvania Sub-Class by representing that it did
20 and would comply with the requirements of relevant federal and state laws pertaining to the
21 privacy and security of the alternative Pennsylvania Sub-Class's Personal and Medical
22 Information in violation of 73 Pa. Stat. Ann. § 201-2(4)(v), (ix), and (xxi);

23 c. Defendant omitted, suppressed, and concealed the material fact of the
24 inadequacy of the privacy and security protections for the alternative Pennsylvania Sub-
25 Class's Personal and Medical Information in violation of in violation of 73 Pa. Stat. Ann. §
26 201-2(4)(v), (ix), and (xxi);

27 d. Defendant engaged in unfair, unlawful, and deceptive acts and practices
28 with respect to the sale of products and services by failing to maintain the privacy and

1 security of the alternative Pennsylvania Sub-Class's Personal and Medical Information, in
2 violation of duties imposed by and public policies reflected in applicable federal and state
3 laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices
4 violated duties imposed by laws including the FTC Act, 15 U.S.C. § 45 and HIPAA, 42 U.S.C.
5 § 1302d, *et seq.*;

6 e. Defendant engaged in unlawful, unfair, and deceptive acts and practices
7 with respect to the sale of products and services by failing to disclose the Data Breach to the
8 alternative Pennsylvania Sub-Class in a timely and accurate manner, in violation of 73 Pa.
9 Stat. § 2303(a); and

10 f. Defendant engaged in unlawful, unfair, and deceptive acts and practices
11 with respect to the sale of products and services by failing to take proper action following
12 the Data Breach to enact adequate privacy and security measures and protect the alternative
13 Pennsylvania Sub-Class's Personal and Medical Information from further unauthorized
14 disclosure, release, data breach, and theft.

15 220. The above unlawful, unfair, and deceptive acts and practices by Defendant
16 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
17 to consumers that the consumers could not reasonably avoid; this substantial injury
18 outweighed any benefits to consumers or to competition.

19 221. Defendant knew or should have known that its computer systems and data
20 security practices were inadequate to safeguard the alternative Pennsylvania Sub-Class'
21 Personal and Medical Information and that risk of a data breach or theft was highly likely.
22 Defendant's actions in engaging in the above-named deceptive acts and practices were
23 negligent, knowing and willful, and/or wanton and reckless with respect to the rights of
24 members of the alternative Pennsylvania Sub-Class.

25 222. Defendant intended for Plaintiff and the alternative Pennsylvania Sub-Class to
26 rely on, and they did rely on, Defendant's misrepresentations and omissions of material fact
27 as alleged herein.

1 223. As a direct and proximate result of Defendant's deceptive acts and practices,
2 the alternative Pennsylvania Sub-Class Members suffered an ascertainable loss of money or
3 property and actual damages, as described above, including the loss of their legally protected
4 interest in the confidentiality and privacy of their Personal and Medical Information.

5 224. Plaintiff and the alternative Pennsylvania Sub-Class seek relief under 73 Pa.
6 Cons. Stat. §201-9.2, including injunctive relief, actual damages, \$100 statutory damages per
7 Class member, and/or treble damages, whichever is greater, along with reasonable attorney
8 fees and costs.

9 **COUNT XII**

10 **INJUNCTIVE / DECLARATORY RELIEF**

11 225. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

12 226. This count is brought on behalf of all Classes.

13 227. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C.
14 §2201.

15 228. As previously alleged, Plaintiff and Class Members entered into an implied
16 contract that required Defendant to provide adequate security for the Personal and Medical
17 Information it collected from Plaintiff and Class Members.

18 229. Defendant owes a duty of care to Plaintiff and Class Members requiring it to
19 adequately secure Personal and Medical Information.

20 230. Defendant still possess Personal and Medical Information regarding Plaintiff
21 and Class Members.

22 231. Since the Data Breach, Defendant has announced few if any changes to its data
23 security infrastructure, processes or procedures to fix the vulnerabilities in its computer
24 systems and/or security practices which permitted the Data Breach to occur and go
25 undetected for years and, thereby, prevent further attacks.

26 232. Defendant has not satisfied its contractual obligations and legal duties to
27 Plaintiff and Class Members. In fact, now that Defendant's insufficient data security is
28

1 known to hackers, the Personal and Medical Information in Defendant's possession is even
2 more vulnerable to cyberattack.

3 233. Actual harm has arisen in the wake of the Data Breach regarding Defendant's
4 contractual obligations and duties of care to provide security measures to Plaintiff and Class
5 Members. Further, Plaintiff and Class Members are at risk of additional or further harm due
6 to the exposure of their Personal and Medical Information and Defendant's failure to
7 address the security failings that lead to such exposure.

8 234. There is no reason to believe that Defendant's security measures are any more
9 adequate now than they were before the breach to meet Defendant's contractual obligations
10 and legal duties.

11 235. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security
12 measures do not comply with its contractual obligations and duties of care to provide
13 adequate security, and (2) that to comply with its contractual obligations and duties of care,
14 Defendant must implement and maintain reasonable security measures, including, but not
15 limited to:

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

21 b. Ordering that Defendant engage third-party security auditors and
22 internal personnel to run automated security monitoring;

23 c. Ordering that Defendant audit, test, and train its security personnel
24 regarding any new or modified procedures;

25 d. Ordering that Defendant segment customer data by, among other
26 things, creating firewalls and access controls so that if one area of Defendant's systems is
27 compromised, hackers cannot gain access to other portions of Defendant's systems;

1 e. Ordering that Defendant not transmit Personal and Medical
2 Information via unencrypted email;

3 f. Ordering that Defendant not store Personal and Medical Information in
4 email accounts;

5 g. Ordering that Defendant purge, delete, and destroy in a reasonably
6 secure manner customer data not necessary for its provisions of services;

7 h. Ordering that Defendant conduct regular database scanning and
8 securing checks;

9 i. Ordering that Defendant routinely and continually conduct internal
10 training and education to inform internal security personnel how to identify and contain a
11 breach when it occurs and what to do in response to a breach; and

12 j. Ordering Defendant to meaningfully educate its current, former, and
13 prospective patients about the threats they face as a result of the loss of their Personal and
14 Medical Information to third parties, as well as the steps they must take to protect
15 themselves.

16 **PRAYER FOR RELIEF**

17 Plaintiff, on behalf of himself and the Classes, respectfully requests the Court order
18 relief and enter judgment in their favor and against Sunshine as follows:

19 A. An order certifying this action as a class action under Fed. R. Civ. P. 23,
20 defining the Classes as requested herein, appointing the undersigned as Class counsel, and
21 finding that Plaintiff is a proper representative of the Classes requested herein.

22 B. Plaintiff requests injunctive and other equitable relief as is necessary to protect
23 the interests of the Classes, including (i) an order prohibiting Defendant from engaging in
24 the wrongful and unlawful acts described herein; (ii) requiring Defendant to protect all data
25 collected or received through the course of its business in accordance with HIPAA
26 regulations, the CMIA, the CCRA, other federal, state and local laws, and best practices
27 under industry standards; (iii) requiring Defendant to design, maintain, and test its computer
28 systems to ensure that Personal and Medical Information in its possession is adequately

1 secured and protected; (iv) requiring Defendant to disclose any future data breaches in a
2 timely and accurate manner; (v) requiring Defendant to engage third-party security auditors
3 as well as internal security personnel to conduct testing, including simulated attacks,
4 penetration tests, and audits on Defendant's systems on a periodic basis and ordering it to
5 promptly correct any problems or issues detected by these auditors; (vi) requiring Defendant
6 to audit, test, and train its security personnel to run automated security monitoring,
7 aggregating, filtering and reporting on log information in a unified manner; (vii) requiring
8 Defendant to implement multi-factor authentication requirements; (viii) requiring
9 Defendant's employees to change their passwords on a timely and regular basis, consistent
10 with best practices; (ix) requiring Defendant to encrypt all Personal and Medical Information;
11 (x) requiring Defendant to audit, test, and train its security personnel regarding any new or
12 modified procedures; (xi) requiring Defendant to segment data by, among other things,
13 creating firewalls and access controls so that if one area of Defendant's network is
14 compromised, hackers cannot gain access to other portions of Defendant's systems; (xii)
15 requiring Defendant to purge, delete, and destroy in a reasonably secure and timely manner
16 Personal and Medical Information no longer necessary for the provision of services; (xiii)
17 requiring Defendant to conduct regular database scanning and securing checks; (xiv)
18 requiring Defendant to routinely and continually conduct internal training and education to
19 inform internal security personnel how to identify and contain a breach when it occurs and
20 what to do in response to a breach; (xv) requiring Defendant to provide lifetime credit
21 monitoring and identity theft repair services to Class Members; and (xvi) requiring
22 Defendant to educate all Class Members about the threats they face as a result of the loss of
23 their Personal and Medical Information to third parties, as well as steps Class Members must
24 take to protect themselves.

25 C. A judgment awarding Plaintiff and Class Members appropriate monetary relief,
26 including actual damages, punitive damages, treble damages, statutory damages, exemplary
27 damages, equitable relief, restitution, and disgorgement;

- 1 D. An order that Defendant pay the costs involved in notifying the Class Members
2 about the judgment and administering the claims process;
- 3 E. Pre-judgment and post-judgment interest;
- 4 F. Attorneys' fees, expenses, and the costs of this action; and
- 5 G. All other and further relief as this Court deems necessary, just, and proper.

6 **JURY DEMAND**

7 Plaintiff demands a trial by jury on all issues so triable.

8 Respectfully submitted,

9
10 DATED: March 10, 2020

11 /s/ Tina Wolfson
12 Tina Wolfson
13 Bradley K. King
14 **AHDOOT & WOLFSON, PC**
15 10728 Lindbrook Drive
16 Los Angeles, CA 90024
17 Tel: (310) 474-9111; Fax: (310) 474-8585

18 Cornelius P. Dukelow*
19 **ABINGTON COLE + ELLERY**
20 320 South Boston Avenue
21 Suite 1130
22 Tulsa, Oklahoma 74103
23 918.588.3400 (*telephone & facsimile*)
24 cdukelow@abingtonlaw.com

25 *Pro Hac Vice application to be submitted

26 *Counsel for Plaintiff*

EXHIBIT 1

ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call: (833) 719-0129 Or Visit: https://ide.myidcare.com/sbhg Enrollment Code: <<XXXXXXXX>>
--

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>,

Sunshine Behavioral Health Group, LLC (“Sunshine”) is writing to notify you of an event that may have affected the security of some of your personal information. Sunshine provides business services to several health care providers, including Monarch Shores, Chapters Capistrano, Willow Springs Recovery and Mountain Springs. This letter provides details of the incident, our response, and resources available to you. We are not aware of any malicious misuse of your personal information, but we are notifying you out of an abundance of caution so you can take steps to help safeguard your personal information, should you feel it is appropriate to do so.

What Happened?

On September 4, 2019, Sunshine became aware that a cloud-based system used to store certain patient records on behalf of the above health care providers was inadvertently set-up in such a manner that permitted the records to be made available on the Internet. Sunshine immediately took steps to change the settings, and, on November 14, 2019, took additional actions to remove the records from general Internet access. Sunshine confirmed that personal information was affected by the incident, and began an investigation to identify the affected individuals and types of personal information involved. Through our investigation, on December 23, 2019, we learned that some personal information related to you was stored in the affected system. Your personal information may have been in our records because you paid for health care services on behalf of a patient.

What Information Was Involved?

Our ongoing investigation confirmed the personal information present in the impacted storage folder may have included contact information, such as your name and address; credit or debit card number, as well as the expiration date and/or security code; and an electronic or digital signature.

What We Are Doing.

Upon learning of this incident, we immediately took steps to address the incident and confirm the security of our systems. We modified access controls for the affected system and reviewed our company policies and procedures relating to the security and privacy of patient records. We are also notifying affected individuals, including you, so that you may take further steps to best safeguard your personal information, should you feel it is appropriate to do so. To that end, we are working with ID Experts to offer MyIDCare protection for 24 months at no cost to you. MyIDCare protection is explained in more detail below.



What You Can Do.

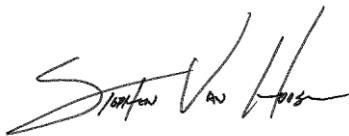
You may review the information contained in the attached document titled “Recommended Steps to Help Protect Your Information.” We also encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (833) 719-0129 or going to <https://ide.myidcare.com/sbhg> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 9:00 a.m. to 9:00 p.m., EST. Please note that the deadline to enroll is April 24, 2020. We encourage you to take full advantage of this service offering.

For More Information.

We recognize that you may have questions not addressed in this letter. If so, we encourage you to call our dedicated assistance line at (833) 719-0129 (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m., EST.

For more detailed instructions on signing up for the MyIDCare protection, please review the attached “Recommended Steps to Help Protect Your Information” document. Note that you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this document. Please call (833) 719-0129 or go to <https://ide.myidcare.com/sbhg> for assistance or for any additional questions you may have regarding MyIDCare.

Sincerely,

A handwritten signature in black ink, appearing to read "Stephen Van Hooser". The signature is stylized and written in cursive.

Stephen Van Hooser
Director of Compliance

(Enclosure)



Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Go to <https://ide.myidcare.com/sbhg> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.
- 3. Telephone.** Contact MyIDCare at (833) 719-0129 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you are entitled to one free copy of your credit report from each of the three major credit reporting companies every 12 months. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop, and reverse any damage quickly.

You should also know that you have the right to file a police report if you ever experience identity theft. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but it may also delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order credit reports from all three bureaus, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning the identity theft.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, KY 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing to the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, Telephone: 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.