

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

IN THE UNITED STATE DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

ALAN HALL, individually and on behalf of all
others similarly situated,

Plaintiffs,

v.

SEA MAR COMMUNITY HEALTH
CENTERS,

Defendants.

Case No.

NOTICE OF REMOVAL OF ACTION
UNDER 28 USC § 1346(b)(1)

(Clerk’s Action Required)

King County Superior Court
Case No. 21-2-15130-9 SEA

TO: THE CLERK OF THE COURT

AND TO: ALL PARTIES OF RECORD AND THEIR COUNSEL.

PLEASE TAKE NOTICE that Defendant SEA MAR COMMUNITY HEALTH CENTERS (“Sea Mar”), hereby gives notice of the removal of the above-captioned action, Cause No. 21-2-15-130-9 SEA, currently pending in the Superior Court of King County, Washington, to the United States District Court for the Western District of Washington at Seattle on the grounds set forth below:

I. STATE COURT ACTION

The State Court action to be removed, *Alan Hall, individually and on behalf of all others similarly situated v. Sea Mar Community Health Centers*, was filed in King County Superior

1 Court, State of Washington, on November 11, 2021. A true and correct copy of the Class Action
2 Complaint filed in King County Superior Court Case No: 21-2-15-130-9 SEA is filed herewith as
3 **Exhibit A**. This is a civil action arising out of alleged violations of (1) RCW 70.02.005,
4 Washington State Uniform Healthcare Information Act, and (2) RCW 19.86.010, Washington
5 State Consumer Protection Act; as well as allegations of (3) negligence, (4) breach of express
6 contract; (5) breach of implied contract; and (6) breach of confidence, with claims made by
7 Plaintiffs for actual damages, compensatory damages, statutory penalties, disgorgement,
8 restitution, credit monitoring, punitive damages, injunctive relief regarding notices and security
9 practices, attorney fees and costs, and pre- and post-judgment interest.

10 **II. GROUNDS FOR REMOVAL**

11 The Federally Supported Health Centers Assistance Act allows the United States to deem
12 actors, agencies, and employees to be part of the Public Health Service.

13 **A. Sea Mar is a Deemed Employee of the Federal Government.**

14 Sea Mar is a community-based health care provider that receives funds from the Health
15 Resources & Services Administration. Sea Mar receives government funding because it provides
16 primary care services in underserved areas. Sea Mar is a Federally Qualified Health Center. As
17 such, Sea Mar has been deemed by the Health Resources and Services Administration, in
18 accordance with the Federally Supported Health Centers Assistance Act, to be a Public Health
19 Service employee of the federal government. The relevant deeming notices are attached
20 collectively as **Exhibit B**.

21 **B. The Federal Tort Claims Act, 28 U.S.C. 1346(b) Applies to Plaintiffs’ 22 Claims.**

23 The Federal Tort Claims Act (“FTCA”), 28 U.S.C. § 1346(b) *et seq.*, provides immunity
24 from suits to Sea Mar because Sea Mar has been deemed to be a Public Health Service employee
25 of the federal government.

26 Subject to the provisions of chapter 171 of this title, the district
27 courts . . . shall have exclusive jurisdiction of civil actions against
the United States . . . for injury or loss of property, or personal
injury or death caused by the negligent or wrongful act or omission

1 of any employee of the Government while acting within the scope
2 of his office or employment, under circumstances where the United
3 States, if a private person, would be liable to the claimant in
accordance with the law of the place where the act or omission
occurred.

4 The regulations establish that the federal government is proper party defendant in an
5 FTCA suit and not Public Health Service employees like Sea Mar.

6 **C. The Public Health Services Act Applies to Sea Mar.**

7 The Public Health Service Act provides liability protection to Public Health Service
8 (“PHS”) employees like Sea Mar under the Federal Tort Claims Act, 28 U.S.C. §§ 1346(b). Sea
9 Mar is a PHS employee under the Federally Supported Health Centers Assistance Act, 42 U.S.C.
10 §§ 233(g)-(n). The *exclusive* remedy for damage for personal injury “resulting from the
11 performance of medical, surgical, dental, or *related functions*, ...by any commissioned ...
12 employee of the Public Health Service while acting within the scope of his office or
13 employment” is *against the United States*. 42 U.S.C. § 233(a). Plaintiffs allege they suffered
14 personal injuries, including anxiety and emotional distress, as a result of a data breach incident in
15 the Sea Mar environment. The Federally Supported Health Centers Assistance Act (42 U.S.C. §
16 233(a)) provides absolute immunity for PHS employees acting within the scope of their
17 employment. *Hui v. Castaneda*, 559 U.S. 799, 806 (2010).

18 **D. Sea Mar’s Conduct Was Function Required and Related to the Provision**
19 **of Medical Care.**

20 To facilitate medical care, Sea Mar—like any doctor’s office—creates medical records,
21 and collects and maintains personal information from its patients. The maintenance, retention,
22 and security of patients’ records are legally required and “related functions” to the provision of
23 medical care within the scope of federal immunity. Plaintiffs’ claims arise from a data breach
24 event that allegedly allowed access to patients’ personal identifying information (“PII”) and
25 protected health information (“PHI”). Plaintiffs’ alleged injuries therefore undeniably arise out of
26 the “related functions” to medical care—creating and maintaining medical, financial and other
27 personal records of patients and their guarantors. Sea Mar qualifies for immunity, and in an

1 FTCA suit a plaintiff’s exclusive remedy is to proceed in an action against the United States in
2 district court.

3 **III. TIME FOR REMOVAL**

4 There is no time bar for Notice of Removal under the Federal Tort Claims Act 28 U.S.C.
5 §1346(b)(1) because the district courts have exclusive jurisdiction over actions against the
6 United States for negligent or wrongful acts or omissions committed by government employees.
7 “ Subject to the provisions of chapter 171 of this title, the district courts . . . shall have exclusive
8 jurisdiction of civil actions against the United States . . . for injury or loss of property, or
9 personal injury . . .”

10 Pursuant to the Federal Tort Claims Act, 28 U.S.C. §§ 1346(b) and the Federally
11 Supported Health Centers Assistance Act, 42 U.S.C. §§ 233(g)-(n) the district court has
12 exclusive jurisdiction over FTCA claims, and in an FTCA suit the only remedy is against the
13 United States.

14 **IV. REQUIRED DOCUMENTS**

15 Defendant Sea Mar will promptly give written notice to all adverse parties. 28 USC §
16 1446(d).

17 In accordance with 28 USC § 1446 and LCR 101 (b)(1), a copy of the operative
18 complaint is attached and filed herewith as **Exhibit A**.

19 Opposing counsel is listed below and is being served with a copy of this Notice as set
20 forth in the Declaration of Service below in accordance with LCR 101(b)(2).

21 WHEREFORE, Defendant Sea Mar gives notice that the court action pending against it
22 in King County Superior Court has been removed from that court to the United States District
23 Court for the Western District of Washington at Seattle.

24 ///

25 ///

26 ///

27 ///

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

DATED: February 16, 2022

LEWIS BRISBOIS BISGAARD & SMITH LLP

s/Kathleen A. Nelson

Kathleen A. Nelson, WSBA #22826

s/Randy J. Aliment

Randy J. Aliment, WSBA #11440

s/Aryn M. Seiler

Aryn M. Seiler, WSBA #57270

1111 Third Avenue, Suite 2700

Seattle, Washington 98101

(206) 436-2020 / (206)436-2030 Fax

Kathleen.Nelson@lewisbrisbois.com

Randy.Aliment@lewisbrisbois.com

Aryn.Seiler@lewisbrisbois.com

Attorneys for Defendant

DECLARATION OF SERVICE

I hereby declare under penalty of perjury under the laws of the State of Washington that I caused a true and correct copy of the foregoing to be served via the methods below February 16, 2022 on the following counsel/party of record:

5 Michael C. Subit, WSBA #29189 6 FRANK FREED SUBIT & THOMAS LLP 7 705 Second Avenue, Suite 1200 8 Seattle, WA 98104 (206) 682-6711 <i>Attorneys for Plaintiff</i>	<input type="checkbox"/> via U.S. Mail, first class, postage prepaid <input type="checkbox"/> via Legal Messenger Hand Delivery <input type="checkbox"/> via Facsimile <input checked="" type="checkbox"/> via CM/ECF <input checked="" type="checkbox"/> via E-mail: msubit@frankfreed.com
9 Gary E. Mason (<i>pro hac vice</i>) 10 David K. Lietz (<i>pro hac vice</i>) MASON LIETZ & KLINGER LLP 11 5101 Wisconsin Avenue NW, Suite 305 Washington, DC 20016 12 (202) 640-1160 13 Gary M. Klinger (<i>pro hac vice</i>) 14 MASON LIETZ & KLINGER LLP 227 W. Monroe Street, Suite 2100 15 Chicago, IL 60630 (312) 283-3814 16 <i>Attorneys for Plaintiff</i>	<input type="checkbox"/> via U.S. Mail, first class, postage prepaid <input type="checkbox"/> via Legal Messenger Hand Delivery <input type="checkbox"/> via Facsimile <input checked="" type="checkbox"/> via CM/ECF <input checked="" type="checkbox"/> via E-mail: gmason@masonllp.com dlietz@masonllp.com gklinger@masonllp.com
17 Nicholas W. Brown 18 Kristen R. Vogel, NY No. 5195664 Assistant United States Attorney 19 Western District of Washington 700 Stewart Street, Suite 5220 20 Seattle, Washington 98101-1271 (206) 553-7970 / (206) 553-4067 Fax 21 <i>United States Attorneys</i>	<input type="checkbox"/> via U.S. Mail, first class, postage prepaid <input type="checkbox"/> via Legal Messenger Hand Delivery <input type="checkbox"/> via Facsimile <input checked="" type="checkbox"/> via CM/ECF <input checked="" type="checkbox"/> via E-mail: kristen.vogel@usdoj.gov

Dated February 16, 2022 at Seattle, Washington.

s/ Annie Kliemann

 Annie Kliemann
Annie.Kliemann@lewisbrisbois.com

EXHIBIT A

0300
GEGFAPUXAFGAEKÍÁÚT
SQŌÁUWVŸ
ÙWÚÒÜŦÛÁÛUWÜVÁŠÒÜS
ÒÈZŠÖÖ
ÔÈÛÒÁKŸFÈĚÍFHEÛÁÛÖE

**IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THE COUNTY OF KING**

ALAN HALL, individually and on behalf of all
others similarly situated,

Plaintiffs,

v.

SEA MAR COMMUNITY HEALTH
CENTERS,

Defendant.

Cause No.

CLASS ACTION COMPLAINT

CLASS ACTION COMPLAINT

Plaintiff Alan Hall, individually, and on behalf of all others similarly situated, brings this action against Defendant Sea Mar Community Health Centers (“SMCHC” or “Defendant”), a Washington corporation,” to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. SMCHC is a health-care provider that provides medical services to patients in the State of Washington.

1 2. Between the dates of December 2020 and March 2021, an unauthorized individual
2 hacked SMCHC’s IT network and obtained unauthorized access to confidential files containing
3 current and former patients’ Private Information (the “Data Breach”).

4 3. For at least three months, the cybercriminals who hacked into SMCHC’s IT
5 network had unfettered access to files containing information pertaining to SMCHC patients (like
6 Plaintiff).

7 4. Incredibly, the threat actor—known as the “Marketo gang”—stole 3 TB of sensitive
8 data from SMCHC and thereafter posted it for sale on the “Marketo marketplace,” a marketplace
9 where the cybercriminals sell their stolen data to the highest bidder on the dark web.
10

11 5. Defendant only became aware of the hacking incident and Data Breach on June 24,
12 2021, when the unauthorized actor informed Defendant that it had successfully copied the sensitive
13 data from its digital environment.
14

15 6. As a result of the Data Breach, Plaintiff and more than 650,000 Class Members
16 suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and
17 identity theft, loss of the benefit of their bargain, out-of-pocket expenses and the value of their
18 time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of value of
19 their personal information.
20

21 7. In addition, Plaintiff’s and Class Members’ sensitive personal information—which
22 was entrusted to Defendant—was compromised and unlawfully accessed due to the Data Breach.

23 8. Information compromised in the Data Breach includes patient names, addresses,
24 dates of birth, Social Security numbers, medical and clinical treatment information, insurance
25 information, claims information and other protected health information as defined by the Health
26

1 Insurance Portability and Accountability Act of 1996 (“HIPAA”) that Defendant collected and
2 maintained (collectively the “Private Information”).

3 9. SMCHC did not notify patients’ that their Private Information was subject to
4 unauthorized access in the Data Breach until October 2021, approximately ten (10) months after
5 the cyberattack was launched and approximately four (4) months after the Data Breach discovered.
6

7 10. The Data Breach was a direct result of Defendant’s failure to implement adequate
8 and reasonable cyber-security procedures and protocols necessary to protect patients’ and
9 employees’ Private Information.

10 11. Plaintiff brings this class action lawsuit on behalf of those similarly situated to
11 address Defendant’s inadequate safeguarding of Class Members’ Private Information that
12 Defendant collected and maintained, and for failing to provide timely and adequate notice to
13 Plaintiff and other Class Members that their information had been subject to the unauthorized
14 access of an unknown third party.
15

16 12. Defendant SMCHC maintained the Private Information in a reckless manner. In
17 particular, the Private Information was maintained on Defendant’s computer network in a
18 condition vulnerable to cyberattacks.

19 13. Upon information and belief, the mechanism of the hacking and potential for
20 improper disclosure of Plaintiff’s and Class Members’ Private Information was a known risk to
21 Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the
22 Private Information from those risks left that property in a dangerous condition.
23

24 14. Defendant disregarded the rights of Plaintiff and Class Members (defined below)
25 by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and
26

1 reasonable measures to ensure its data systems were protected against unauthorized intrusions;
2 failing to disclose that it did not have adequately robust computer systems and security practices
3 to safeguard patient Private Information; failing to take standard and reasonably available steps to
4 prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt notice of the
5 Data Breach.

6
7 15. In addition, Defendant and its employees failed to properly monitor the computer
8 network and systems that housed the Private Information. Had Defendant properly monitored its
9 property, it would have discovered the intrusion sooner, as opposed to letting cyberthieves roam
10 freely in Defendant's IT network for four (4) months.

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

14
15 17. Armed with the Private Information accessed in the Data Breach, data thieves can
16 commit a variety of crimes including, e.g., opening new financial accounts in Class Members'
17 names, taking out loans in Class Members' names, using Class Members' names to obtain medical
18 services, using Class Members' information to obtain government benefits, filing fraudulent tax
19 returns using Class Members' information, obtaining driver's licenses in Class Members' names
20 but with another person's photograph, and giving false information to police during an arrest.

21
22 18. As a result of the Data Breach, Plaintiff and Class Members have been exposed to
23 a present and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and
24 in the future closely monitor their financial accounts to guard against identity theft.

25 19. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing
26

1 credit monitoring services, credit freezes, credit reports, or other protective measures to deter and
2 detect identity theft.

3 20. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated
4 individuals whose Private Information was accessed during the Data Breach.

5 21. Plaintiff seeks remedies including, but not limited to, compensatory damages,
6 nominal damages, reimbursement of out-of-pocket costs, and injunctive relief including
7 improvements to SMCHC's data security systems, future annual audits, and adequate credit
8 monitoring services funded by Defendant.
9

10 **PARTIES**

11 22. Plaintiff Alan Hall is, and at all times mentioned herein was, an individual citizen
12 of the State of Washington residing in the City of Bellingham. Plaintiff was a patient at SMCHC
13 and received medical services and treatments from same. Plaintiff was notified of Defendant's
14 Data Breach and his Private Information being compromised upon receiving a notice letter dated
15 October 26, 2021.
16

17 23. Defendant SMCHC is a health-care services provider with its principal place of
18 business at 1040 S. Henderson Street, Seattle, WA, 98108.
19

20 **JURISDICTION AND VENUE**

21 24. This Court has jurisdiction over Defendant because Defendant is organized under
22 the laws of the State of Washington and the causes of action alleged herein arise from Defendant
23 transacting business in Washington.

24 25. Venue is proper in this Court as a substantial portion of the acts and transactions
25 that constitute violations of law complained of herein occurred in King County and Defendant
26

1 conducts substantial business throughout King County.

2 **DEFENDANT'S BUSINESS**

3 26. Defendant SMCHC is an organization that provides health, human, housing,
4 educational and cultural services to communities in the State of Washington.

5 27. In the ordinary course of receiving treatment and health care services from
6 SMCHC, patients are required to provide sensitive personal and private information such as:
7

- 8 • Names;
- 9 • Dates of birth;
- 10 • Social Security numbers;
- 11 • Driver's license numbers;
- 12 • Financial account information;
- 13 • Payment card information;
- 14 • Medical histories;
- 15 • Treatment information;
- 16 • Medication or prescription information;
- 17 • Beneficiary information;
- 18 • Address, phone number, and email address, and;
- 19 • Health insurance information, including health insurance plan member IDs.

20 28. Prior to receiving care and treatment from SMCHC, Plaintiff was required to and
21 did in fact turn over much (if not all) of the private and confidential information listed above.

22 29. Additionally, SMCHC may receive private and personal information from other
23 individuals and/or organizations that are part of a patient's "circle of care," such as referring
24
25
26

1 physicians, patients' other doctors, patient's health plan(s), close friends, and/or family members.

2 30. SMCHC also creates and maintains a considerable amount of Protected Health
3 Information (PHI) in the course of providing medical care and treatment.

4 31. On information and belief, SMCHC provides each of its patients with a HIPAA
5 compliant notice of its privacy practices (the "Privacy Notice") in respect to how they handle
6 patients' sensitive and confidential information.

7 32. A copy of the Privacy Notice is maintained on SMCHC's website, and may be
8 found here: <https://www.seamar.org/notice.html>.

9 33. Due to the highly sensitive and personal nature of the information SMCHC acquires
10 and stores with respect to its patients, SMCHC recognizes patients' Rights to Privacy in its Privacy
11 Notice, and promises in its Privacy Notice, to, among other things, maintain the privacy of patients'
12 protected health information.

13 34. SMCHC promises to maintain the confidentiality of patients' health, financial, and
14 non-public personal information, ensure compliance with federal and state laws and regulations,
15 and not to use or disclose patients' health information for any reasons other than those expressly
16 listed in the Privacy Notice without written authorization.

17 35. As a condition of receiving medical care and treatment at Defendant's facilities,
18 Defendant requires that each of its patients (including Plaintiff) sign a Notice of Privacy Practices
19 Acknowledgment, which can be found here: [https://www.seamar.org/seamar-](https://www.seamar.org/seamar-downloads/covid/PatientAcknow_ENG.pdf)
20 [downloads/covid/PatientAcknow_ENG.pdf](https://www.seamar.org/seamar-downloads/covid/PatientAcknow_ENG.pdf).

21 36. Upon information and belief, Plaintiff did in fact sign a Notice of Privacy Practices
22 Acknowledgment prior to receiving care or treatment from Defendant.
23
24
25
26

- i. Marketo has been observed sending samples of compromised data to the competitors, clients, and partners of their victims.
- ii. Marketo publicly shames organizations that have not contacted the group stating the organization does not care about data security.
- iii. Marketo will share subsets of data with victims as a way to prove the validity of their claims.
- iv. Marketo publishes data incrementally until all information is public.²

44. The Marketo gang also offers up for sale the stolen data they steal on their marketplace, selling the sensitive data to the highest bidder on the Dark Web.³

45. Consistent with the Marketo gang's *modus operandi* of exfiltrating and stealing data, SMCHC admits that the unauthorized party "copied" the sensitive data "from its digital environment."⁴

46. Indeed, following the Data Breach, the prized data was posted on Marketo's marketplace for sale to cybercriminals, as depicted in the following image⁵:

² <https://www.digitalshadows.com/blog-and-research/marketo-a-return-to-simple-extortion/>.

³ <https://thedigitalhacker.com/irony-at-its-peak-marketo-gang-claims-to-have-bids-on-stolen-data-of-an-it-service-company-fujitsu/>.

⁴ <https://www.prnewswire.com/news-releases/sea-mar-community-health-centers-provides-notice-of-data-security-incident-301412308.html>.

⁵ <https://www.databreaches.net/wa-sea-mar-community-health-centers-discloses-breach-that-began-last-year/>.



47. The information stolen in the Data Breach included patient names, address, Social Security number, date of birth, client identification number, medical / vision / dental / orthodontic diagnostic and treatment information, medical / vision / dental insurance information, claims information, and / or images associated with dental treatment.

48. The Private Information contained in the files accessed by hackers was not encrypted.

49. Upon information and belief, the Data Breach was targeted at Defendant due to its status as a healthcare entity that collects, creates, and maintains both PII and PHI.

50. Upon information and belief, the targeted Data Breach was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII and PHI of patients, like Plaintiff and the Class Members.

51. While SMCHC stated in notice letters sent to Plaintiff and Class Members (as well

1 as on its website) that it learned of the Ransomware Attack on June 24, 2021, SMCHC did not
2 begin notifying impacted patients, such as Plaintiff and Class Members, until October 2021 –
3 nearly 4 months after discovering the Data Breach.

4 52. Defendant SMCHC admits that its cybersecurity practices were inadequate. Indeed
5 SMCHC admits that it is now taking the appropriate “steps to prevent a similar incident from
6 occurring in the future,” which is an implicit admission these security measures were not in place
7 to begin with. Moreover, SMCHC stated that it “deeply regrets” that any inconvenience the Data
8 Breach caused Plaintiff and Class Members.⁶

9 10 53. Due to Defendant’s incompetent security measures, Plaintiff and the Class
11 Members now face a present and immediate risk of fraud and identity theft and must deal with that
12 threat forever.

13 14 54. Plaintiff believes his Private Information was stolen in the Data Breach and that
15 said information was subsequently posted for sale on the dark web following the Data Breach, as
16 that is the *modus operandi* of all cybercriminals, and especially the Marketo gang.

17 18 55. Defendant had obligations created by HIPAA, contract, industry standards,
19 common law, and its own promises and representations made to Plaintiff and Class Members to
20 keep their Private Information confidential and to protect it from unauthorized access and
21 disclosure.

22 23 56. Plaintiff and Class Members provided their Private Information to Defendant with
24 the reasonable expectation and mutual understanding that Defendant would comply with its

25
26 ⁶ <https://www.prnewswire.com/news-releases/sea-mar-community-health-centers-provides-notice-of-data-security-incident-301412308.html>.

1 obligations to keep such information confidential and secure from unauthorized access.

2 57. Defendant's data security obligations were particularly important given the
3 substantial increase in ransomware attacks and/or data breaches in the healthcare industry
4 preceding the date of the breach.

5 58. In 2019, a record 1,473 data breaches occurred, resulting in approximately
6 164,683,455 sensitive records being exposed, a 17% increase from 2018.⁷ Of the 1,473 recorded
7 data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.⁸ The 525
8 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157),
9 compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in
10 2018.⁹

11 59. In light of recent high profile cybersecurity incidents at other healthcare partner and
12 provider companies, including, American Medical Collection Agency (25 million patients, March
13 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic
14 Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September
15 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency
16 Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC
17 Health System (286,876 patients, March 2020), Defendant knew or should have known that its
18 electronic records would be targeted by cybercriminals.

19 60. In 2021 alone there have been over 220 data breach incidents.¹⁰ These

20
21
22
23
24 ⁷ https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed June 1, 2021)

25 ⁸ *Id.*

26 ⁹ *Id.* at p15.

¹⁰ See Kim Delmonico, Another (!) Orthopedic Practice Reports Data Breach, Orthopedics This Week (May 24, 2021), <https://ryortho.com/breaking/another-orthopedic-practice-reports-data-breach/>.

1 approximately 220 data breach incidents have impacted nearly 15 million individuals.¹¹

2 61. Indeed, cyberattacks have become so notorious that the Federal Bureau of
3 Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they
4 are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller
5 municipalities and *hospitals* are attractive to ransomware criminals... because they often have
6 lesser IT defenses and a high incentive to regain access to their data quickly.”¹²

7
8 62. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare
9 organizations experienced cyberattacks in the past year.¹³

10 63. Therefore, the increase in such attacks, and attendant risk of future attacks, was
11 widely known to the public and to anyone in Defendant’s industry, including Defendant.

12 ***Defendant Fails to Comply with FTC Guidelines***

13
14 64. The Federal Trade Commission (“FTC”) has promulgated numerous guides for
15 businesses which highlight the importance of implementing reasonable data security practices.
16 According to the FTC, the need for data security should be factored into all business decision-
17 making.

18 65. In 2016, the FTC updated its publication, *Protecting Personal Information: A*
19 *Guide for Business*, which established cyber-security guidelines for businesses. The guidelines
20 note that businesses should protect the personal patient information that they keep; properly
21 dispose of personal information that is no longer needed; encrypt information stored on computer
22

23 _____
24 ¹¹ *Id.*

25 ¹² *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019),
<https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited
26 July 2, 2021).

¹³ *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, Security Magazine (Nov. 23, 2020),
<https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack>.

1 networks; understand their network’s vulnerabilities; and implement policies to correct any
2 security problems.¹⁴ The guidelines also recommend that businesses use an intrusion detection
3 system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating
4 someone is attempting to hack the system; watch for large amounts of data being transmitted from
5 the system; and have a response plan ready in the event of a breach.¹⁵
6

7 66. The FTC further recommends that companies not maintain PII longer than is
8 needed for authorization of a transaction; limit access to sensitive data; require complex passwords
9 to be used on networks; use industry-tested methods for security; monitor for suspicious activity
10 on the network; and verify that third-party service providers have implemented reasonable security
11 measures.
12

13 67. The FTC has brought enforcement actions against businesses for failing to
14 adequately and reasonably protect patient data, treating the failure to employ reasonable and
15 appropriate measures to protect against unauthorized access to confidential consumer data as an
16 unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15
17 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take
18 to meet their data security obligations.
19

20 68. These FTC enforcement actions include actions against healthcare providers like
21 Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708,
22 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s
23 data security practices were unreasonable and constitute an unfair act or practice in violation of
24

25 ¹⁴ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at
https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf
(last visited June 15, 2021).

26 ¹⁵ *Id.*

1 Section 5 of the FTC Act.”)

2 69. Defendant failed to properly implement basic data security practices.

3 70. Defendant’s failure to employ reasonable and appropriate measures to protect
4 against unauthorized access to patients’ PII and PHI constitutes an unfair act or practice prohibited
5 by Section 5 of the FTC Act, 15 U.S.C. § 45.
6

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

10 ***Defendant Fails to Comply with Industry Standards***

11 72. As shown above, experts studying cyber security routinely identify healthcare
12 providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI
13 which they collect and maintain.
14

15 73. Several best practices have been identified that a minimum should be implemented
16 by healthcare providers like Defendant, including but not limited to: educating all employees;
17 strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software;
18 encryption, making data unreadable without a key; multi-factor authentication; backup data, and;
19 limiting which employees can access sensitive data.
20

21 74. Other best cybersecurity practices that are standard in the healthcare industry
22 include installing appropriate malware detection software; monitoring and limiting the network
23 ports; protecting web browsers and email management systems; setting up network systems such
24 as firewalls, switches and routers; monitoring and protection of physical security systems;
25 protection against any possible communication system; training staff regarding critical points.
26

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

8 76. These foregoing frameworks are existing and applicable industry standards in the
9 healthcare industry, and Defendant failed to comply with these accepted standards, thereby
10 opening the door to and causing the Ransomware Attack.

11 ***Defendant’s Conduct Violates HIPAA and Evidences Its Insufficient Data Security***

12 77. HIPAA requires covered entities such as Defendant to protect against reasonably
13 anticipated threats to the security of sensitive patient health information.
14

15 78. Covered entities must implement safeguards to ensure the confidentiality, integrity,
16 and availability of PHI. Safeguards must include physical, technical, and administrative
17 components.
18

19 79. Title II of HIPAA contains what are known as the Administrative Simplification
20 provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the
21 Department of Health and Human Services (“HHS”) create rules to streamline the standards for
22 handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple
23 regulations under authority of the Administrative Simplification provisions of HIPAA. These rules
24 include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45
25 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).
26

1 80. A breach such as the one Defendant experienced, is also considered a breach under
2 the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

3 A breach under the HIPAA Rules is defined as, "...the acquisition,
4 access, use, or disclosure of PHI in a manner not permitted under
5 the [HIPAA Privacy Rule] which compromises the security or
6 privacy of the PHI." *See* 45 C.F.R. 164.40

7 81. Defendant's Data Breach resulted from a combination of insufficiencies that
8 demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

9 **DEFENDANT'S BREACH**

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

- 14 a. Failing to maintain an adequate data security system to reduce the risk of data
15 breaches, cyber-attacks, hacking incidents, and ransomware attacks;
- 16 b. Failing to adequately protect patients' Private Information;
- 17 c. Failing to properly monitor its own data security systems for existing or prior
18 intrusions;
- 19 d. Failing to ensure the confidentiality and integrity of electronic PHI it created,
20 received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- 21 e. Failing to implement technical policies and procedures for electronic information
22 systems that maintain electronic PHI to allow access only to those persons or
23 software programs that have been granted access rights in violation of 45 C.F.R. §
24 164.312(a)(1);
25
26

- 1 f. Failing to implement policies and procedures to prevent, detect, contain, and correct
2 security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- 3 g. Failing to implement procedures to review records of information system activity
4 regularly, such as audit logs, access reports, and security incident tracking reports
5 in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- 6 h. Failing to protect against reasonably anticipated threats or hazards to the security
7 or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- 8 i. Failing to protect against reasonably anticipated uses or disclosures of electronic
9 PHI that are not permitted under the privacy rules regarding individually
10 identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- 11 j. Failing to ensure compliance with HIPAA security standard rules by its workforces
12 in violation of 45 C.F.R. § 164.306(a)(4);
- 13 k. Failing to train all members of its workforces effectively on the policies and
14 procedures regarding PHI as necessary and appropriate for the members of its
15 workforces to carry out their functions and to maintain security of PHI, in violation
16 of 45 C.F.R. § 164.530(b);
- 17 l. Failing to render the electronic PHI it maintained unusable, unreadable, or
18 indecipherable to unauthorized individuals, as it had not encrypted the electronic
19 PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process
20 to transform data into a form in which there is a low probability of assigning
21 meaning without use of a confidential process or key” (45 CFR § 164.304’s
22 definition of “encryption”);
23
24
25
26

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

3 n. Failing to adhere to industry standards for cybersecurity.

4 83. As the result of computer systems in need of security upgrades, inadequate
5 procedures for handling email phishing attacks, viruses, malignant computer code, and hacking
6 attacks, SMCHC negligently and unlawfully failed to safeguard Plaintiff's and Class Members'
7 Private Information.
8

9 84. Accordingly, as outlined below, Plaintiff and Class Members now face a present,
10 increased, and immediate risk of fraud and identity theft. In addition, Plaintiff and the Class
11 Members also lost the benefit of the bargain they made with Defendant because of its inadequate
12 data security practices for which they gave good and valuable consideration.
13

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

16 85. Hacking incidents and data breaches at medical facilities like SMCHC are
17 especially problematic because of the disruption they cause to the medical treatment and overall
18 daily lives of patients affected by the attack.

19 86. Researchers have found that at medical facilities that experienced a data security
20 incident, the death rate among patients increased in the months and years after the attack.¹⁶

21 87. Researchers have further found that at medical facilities that experienced a data
22 security incident, the incident was associated with deterioration in timeliness and patient outcomes,
23
24

25 ¹⁶ See Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct.
26 24, 2019), <https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks>.

1 generally.¹⁷

2 88. The United States Government Accountability Office released a report in 2007
3 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face
4 “substantial costs and time to repair the damage to their good name and credit record.”¹⁸

5 89. That is because any victim of a data breach is exposed to serious ramifications
6 regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable
7 information is to monetize it. They do this by selling the spoils of their cyberattacks on the black
8 market to identity thieves who desire to extort and harass victims, take over victims’ identities in
9 order to engage in illegal financial transactions under the victims’ names.
10

11 90. Because a person’s identity is akin to a puzzle, the more accurate pieces of data an
12 identity thief obtains about a person, the easier it is for the thief to take on the victim’s identity, or
13 otherwise harass or track the victim. For example, armed with just a name and date of birth, a data
14 thief can utilize a hacking technique referred to as “social engineering” to obtain even more
15 information about a victim’s identity, such as a person’s login credentials or Social Security
16 number. Social engineering is a form of hacking whereby a data thief uses previously acquired
17 information to manipulate individuals into disclosing additional confidential or personal
18 information through means such as spam phone calls and text messages or phishing emails.
19

20 91. The FTC recommends that identity theft victims take several steps to protect their
21 personal and financial information after a data breach, including contacting one of the credit
22

23 _____
24 ¹⁷ See Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*,
54 Health Services Research 971, 971-980 (2019). Available at
<https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203>.

25 ¹⁸ See U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but*
26 *Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007). Available
at <https://www.gao.gov/new.items/d07737.pdf>.

1 bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone
2 steals their identity), reviewing their credit reports, contacting companies to remove fraudulent
3 charges from their accounts, placing a credit freeze on their credit, and correcting their credit
4 reports.¹⁹

5
6 92. Identity thieves use stolen personal information such as Social Security numbers
7 for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

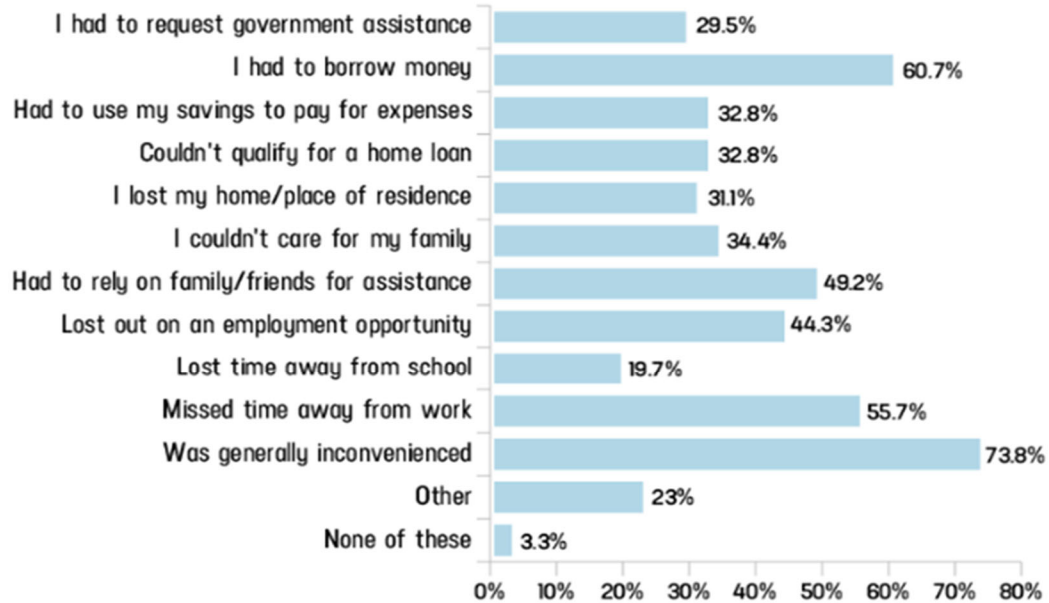
8 93. Identity thieves can also use Social Security numbers to obtain a driver's license or
9 official identification card in the victim's name but with the thief's picture; use the victim's name
10 and Social Security number to obtain government benefits; or file a fraudulent tax return using the
11 victim's information. In addition, identity thieves may obtain a job using the victim's Social
12 Security number, rent a house or receive medical services in the victim's name, and may even give
13 the victim's personal information to police during an arrest resulting in an arrest warrant being
14 issued in the victim's name.
15

16 94. A study by Identity Theft Resource Center shows the multitude of harms caused by
17 fraudulent use of personal and financial information.²⁰
18
19
20
21
22
23
24

¹⁹ See *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/Steps> (last visited Mar. 16, 2021).

²⁰ See Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php>.

Americans' expenses/disruptions as a result of criminal activity in their name [2016]



Source: Identity Theft Resource Center

creditcards.com

95. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.²¹

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

Theft of PHI, in particular, is gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider,

²¹ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

1 or get other care. If the thief’s health information is mixed with yours, your treatment, insurance
2 and payment records, and credit report may be affected.”²²

3
4 97. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and
5 other healthcare service providers often purchase PII and PHI on the black market for the purpose
6 of target marketing their products and services to the physical maladies of the data breach victims
7 themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their
8 insureds’ medical insurance premiums.

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

12
13 99. According to the U.S. Government Accountability Office, which conducted a study
14 regarding data breaches:

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

19 *See* GAO Report, at p. 29.

20 100. Private Information is such a valuable commodity to identity thieves that once the
21 information has been compromised, criminals often trade the information on the “cyber black-
22 market” for years.

23
24 101. There is a strong probability that entire batches of stolen information have been

25
26 ²² *See* Federal Trade Commission, *Medical Identity Theft*, <http://www.consumer.ftc.gov/articles/0171-medical-identity-theft> (last visited Mar. 16, 2021).

1 dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and
2 Class Members are at an increased risk of fraud and identity theft for many years into the future.

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

5 103. Sensitive Private Information can sell for as much as \$363 per record according to
6 the Infosec Institute.²³ PII is particularly valuable because criminals can use it to target victims
7 with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims
8 may continue for years.

9 104. For example, the Social Security Administration has warned that identity thieves
10 can use an individual's Social Security number to apply for additional credit lines.²⁴ Such fraud
11 may go undetected until debt collection calls commence months, or even years, later. Stolen Social
12 Security Numbers also make it possible for thieves to file fraudulent tax returns, file for
13 unemployment benefits, or apply for a job using a false identity.²⁵ Each of these fraudulent
14 activities is difficult to detect. An individual may not know that his or her Social Security Number
15 was used to file for unemployment benefits until law enforcement notifies the individual's
16 employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an
17 individual's authentic tax return is rejected.

18 105. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

19 106. An individual cannot obtain a new Social Security number without significant
20
21
22
23

24 ²³ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),
25 <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>.

²⁴ *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at
26 <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Mar. 16, 2021).

²⁵ *Id* at 4.

1 paperwork and evidence of actual misuse. Even then, a new Social Security number may not be
2 effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the
3 old number, so all of that old bad information is quickly inherited into the new Social Security
4 number.”²⁶

5
6 107. This data, as one would expect, demands a much higher price on the black market.
7 Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card
8 information, personally identifiable information and Social Security Numbers are worth more than
9 10x on the black market.”²⁷

10 108. Medical information is especially valuable to identity thieves.

11 109. According to account monitoring company LogDog, medical data is selling for \$50
12 and up on the Dark Web.²⁸

13
14 110. Because of the value of its collected and stored data, the medical industry has
15 experienced disproportionately higher numbers of data theft events than other industries.

16 111. For this reason, SMCHC knew or should have known about these dangers and
17 strengthened its network and data security systems accordingly. SMCHC was put on notice of the
18 substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for
19 that risk.

20
21
22 ²⁶ Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9,
23 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>.

24 ²⁷ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*,
Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

25 ²⁸ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3,
26 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>.

Plaintiff's and Class Members' Damages

1
2 112. To date, SMCHC has done less than nothing to adequately protect Plaintiff and
3 Class Members, or to compensate them for their injuries sustained in this data breach. Defendant's
4 data breach notice letter completely downplays and disavows the theft of Plaintiff's and Class
5 Members' Private Information, when the facts demonstrate that the Private Information was
6 accessed and exfiltrated. The complimentary identity monitoring service offered by Defendant
7 through Kroll is wholly inadequate as the services are only offered for 12 months and it places the
8 burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for
9 that service, as opposed to automatically enrolling all victims of this cybercrime.
10

11 113. Plaintiff and Class Members have been injured and damaged by the compromise of
12 their Private Information in the Data Breach.
13

14 114. Plaintiff's Private Information (including without limitation his date of birth, Social
15 Security number and medical and insurance information) was compromised in the Data Breach
16 and is now in the hands of the cybercriminals who accessed Defendant's IT network. Class
17 Members' PII and PHI, as described above, was similarly compromised and is now in the hands
18 of the same cyberthieves.
19

20 115. Plaintiff is a current patient of Defendant.

21 116. Plaintiff typically takes measures to protect his Private Information, and is very
22 careful about sharing his PII and PHI. He has never knowingly transmitted unencrypted PII or PHI
23 over the internet or any other unsecured source.

24 117. Plaintiff stores any documents containing his PII and PHI in a safe and secure
25 location. Moreover, he diligently chooses unique usernames and passwords for his online accounts.
26

1 118. To the best of his knowledge, Plaintiff's Private Information was never
2 compromised in any other data breach.

3 119. As a direct and proximate result of Defendant's conduct, Plaintiff and Class
4 Members have been placed at an imminent, immediate, and continuing increased risk of harm from
5 fraud and identity theft.
6

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

9 121. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such
10 as loans opened in their names, tax return fraud, utility bills opened in their names, and similar
11 identity theft.
12

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

17 123. Plaintiff and Class Members may also incur out-of-pocket costs for protective
18 measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in
19 lieu of the inadequate monitoring offered by Defendant), credit report fees, credit freeze fees, and
20 similar costs directly or indirectly related to the Data Breach.
21

22 124. Plaintiff and Class Members also suffered a loss of value of their Private
23 Information when it was acquired by the hacker and cyber thieves in the Data Breach. Numerous
24 courts have recognized the propriety of loss of value damages in related cases.

25 125. Plaintiff and Class Members were also damaged via benefit-of-the-bargain
26

1 damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied
2 by adequate data security but was not. Part of the price Plaintiff and Class Members paid to
3 Defendant was intended to be used by Defendant to fund adequate security of SMCHC's computer
4 property and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the
5 Class Members did not get what they paid for.
6

7 126. Plaintiff and Class Members have spent and will continue to spend significant
8 amounts of time to monitor their financial and medical accounts and records for misuse.

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

- 13 o. Finding fraudulent loans, insurance claims, tax returns, and/or government
14 benefit claims;
- 15 p. Purchasing credit monitoring and identity theft prevention;
- 16 q. Placing "freezes" and "alerts" with credit reporting agencies;
- 17 r. Spending time on the phone with or at a financial institution or government
18 agency to dispute fraudulent charges and/or claims;
- 19 s. Contacting financial institutions and closing or modifying financial accounts;
- 20 t. Closely reviewing and monitoring Social Security Number, medical insurance
21 accounts, bank accounts, and credit reports for unauthorized activity for years
22 to come.
23
24

25 128. Moreover, Plaintiff and Class Members have an interest in ensuring that their
26

1 Private Information, which is believed to remain in the possession of Defendant, is protected from
2 further breaches by the implementation of security measures and safeguards, including but not
3 limited to, making sure that the storage of data or documents containing sensitive and confidential
4 personal, health, and/or financial information is not accessible online, that access to such data is
5 password-protected, and that such data is properly encrypted.
6

7 129. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced
8 to live with the anxiety that their Private Information may be disclosed to the entire world, thereby
9 subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

10 130. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and
11 Class Members have suffered a loss of privacy and are at a present, imminent and increased risk
12 of future harm.
13

14 **CLASS REPRESENTATION ALLEGATIONS**

15 131. Plaintiff brings this action on behalf of herself and on behalf of all other persons
16 similarly situated ("the Class").

17 132. Plaintiff proposes the following Class definition, subject to amendment as
18 appropriate:
19

20 133. All individuals whose Private Information was received, gatherer, shared, obtained,
21 or otherwise found itself in the possession of Defendant and compromised in the Data Breach.

22 134. Excluded from the Class are Defendant's officers, directors, and employees; any
23 entity in which Defendant has a controlling interest; and the affiliates, legal representatives,
24 attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members
25 of the judiciary to whom this case is assigned, their families and members of their staff.
26

1 135. Numerosity. CR 23(a)(1). The members of the Class are so numerous that joinder
2 of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff
3 at this time, based on information and belief, the Class may approach 109,000 patients.

4 136. Commonality. CR 23(a)(2) & (b)(3). There are questions of law and fact common
5 to the Class, which predominate over any questions affecting only individual Class Members.

6 These common questions of law and fact include, without limitation:
7

- 8 a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's
9 and Class Members' Private Information;
- 10 b) Whether Defendant knowingly concealed notification to affected customers of
11 the Data Breach
- 12 c) Whether Defendant unreasonably delayed in notifying affected customers of
13 the Data Breach and whether the belated notice was adequate;
- 14 d) Whether Defendant failed to implement and maintain reasonable security
15 procedures and practices appropriate to the nature and scope of the information
16 compromised in the Data Breach;
- 17 e) Whether Defendant's conduct was negligent;
- 18 f) Whether Defendant violated the requirements of the Washington State
19 Healthcare Information Act, RCW 70.02.005 *et seq.*;
- 20 g) Whether Defendant's acts, inactions, and practices complained of herein
21 violated the Washington State Consumer Protection Act
- 22 h) Whether Defendant breached its contracts (express and implied) for data
23 security and privacy; and
24
25
26

1 i) Whether Plaintiff and Class Members are entitled to damages, treble damages,
2 civil penalties, punitive damages, and/or injunctive relief.

3 137. Typicality. CR 23(a)(3). Plaintiff's claims are typical of those of other Class
4 members because Plaintiff's information, like that of every other Class member, was misused,
5 and/or disclosed by Defendant.

6 138. Adequacy of Representation. CR 23(a)(4). Plaintiff will fairly and adequately
7 represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent
8 and experienced in litigating class actions.

9 139. Superiority of Class Action. CR 23(b)(3). A class action is superior to other
10 available methods for the fair and efficient adjudication of this controversy since joinder of all
11 Class Members is impracticable. Furthermore, the adjudication of this controversy through a class
12 action will avoid the possibility of inconsistent and potentially conflicting adjudication of the
13 asserted claims. There will be no difficulty in the management of this action as a class action.

14 140. Damages for any individual class member are likely insufficient to justify the cost
15 of individual litigation, so that in the absence of class treatment, Defendant's violations of law
16 inflicting substantial damages in the aggregate would go un-remedied without certification of the
17 Class.

18 141. Defendant has acted or refused to act on grounds that apply generally to the Class,
19 as alleged above, and certification is proper under CR 23(b)(2).
20
21
22
23
24
25
26

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

CAUSES OF ACTION

FIRST COUNT

**Violation of the Washington State Uniform Healthcare Information Act
(RCW 70.02.005 *et seq.*)
(On Behalf of Plaintiff and All Class Members)**

142. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

143. Section 70.02.02 of the Revised Code of Washington provides that “Except as authorized elsewhere in this chapter, a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any other person without the patient's written authorization. A disclosure made under a patient's written authorization must conform to the authorization.”

144. At all relevant times, Defendant was a health care provider because it was authorized by the laws of Washington State to provide health care in the ordinary course of their business or practice. RCW 70.02.010(19).

145. At all relevant times, Defendant collected, stored, managed, and transmitted Plaintiff and Class Members’ PII/PHI.

146. Plaintiff and Class Members PII/PHI is “Health Care Information” under RCW 70.02.010(17) in that it identifies or can be readily associated with the identify of a patient and directly relates to the patient’s health care or that it is a required accounting of disclosures of health care information.

147. The Revised Code of Washington requires Defendant to implement and maintain standards of confidentiality with respect to all individually identifiable PHI disclosed to them and

1 maintained by them. Specifically, RCW 70.20.020 prohibits Defendant from disclosing Plaintiff
2 and Class Members' PHI without first obtaining their authorization to do so.

3 148. RCW 70.20.020-030 specifies the manner in which authorization must be obtained
4 before PHI is released. Defendant, however, failed to obtain any authorization—let alone, proper
5 authorization—from Plaintiff and Class Members before releasing and disclosing their PHI. As
6 mandatorily required by RCW 70.20.150 (Security safeguards), Defendant also failed to effect
7 reasonable safeguards for the security of all health care information they maintain, including but
8 not limited to failing to identify, implement, maintain and monitor the proper data security
9 measures, policies, procedures, protocols, and software and hardware systems to safeguard and
10 protect Plaintiff and Class Members' PHI. As a direct and proximate result of Defendant's
11 wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff and Class Members'
12 PHI was disclosed. By disclosing Plaintiff and Class Members' PHI without their written
13 authorization. Defendant violated RCW 70.20.10 *et seq.*, and its legal duty to protect the
14 confidentiality of such information.
15

16
17 149. As a direct and proximate result of Defendant's above-described wrongful actions,
18 inaction, omissions, and want of ordinary care that directly and proximately caused the Data
19 Breach and their violation of the RCW 70.20, pursuant to RCW 70.20.170, Plaintiff and Class
20 Members also are entitled to (1) injunctive relief; (2) actual damages per Plaintiff and each Class
21 member, and; (3) reasonable attorneys' fees and all other expenses.
22

23 **SECOND COUNT**
24 **Violation of the Washington State Consumer Protection Act**
25 **(RCW 19.86.010 *et seq.*)**
26 **(On Behalf of Plaintiff and All Class Members)**

150. Plaintiff repeats and re-alleges each and every factual allegation contained in all

1 previous paragraphs as if fully set forth herein.

2 151. The Washington State Consumer Protection Act, RCW 19.86.020 (the “CPA”)
3 prohibits any “unfair or deceptive acts or practices” in the conduct of any trade or commerce as
4 those terms are described by the CPA and relevant case law.
5

6 152. Defendant is a “person” as described in RWC 19.86.010(1).

7 153. Defendant engages in “trade” and “commerce” as described in RWC 19.86.010(2)
8 in that they engage in the sale of services and commerce directly and indirectly affecting the people
9 of the State of Washington.

10 154. By virtue of the above-described wrongful actions, inaction, omissions, and want
11 of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in
12 unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that
13 Defendant’s practices were injurious to the public interest because they injured other persons, had
14 the capacity to injure other persons, and have the capacity to injure other persons.
15

16 155. In the course of conducting their business, Defendant committed “unfair or
17 deceptive acts or practices” by, *inter alia*, knowingly failing to design, adopt, implement, control,
18 direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies,
19 procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and
20 Class Members’ PII/PHI, and violating the common law alleged herein in the process. Plaintiff
21 and Class Members reserve the right to allege other violations of law by Defendant constituting
22 other unlawful business acts or practices. Defendant’s above described wrongful actions, inaction,
23 omissions, and want of ordinary care are ongoing and continue to this date.
24

25 156. Defendant also violated the CPA by failing to timely notify and concealing from
26

1 Plaintiff and Class Members regarding the unauthorized release and disclosure of their PII/PHI. If
2 Plaintiff and Class Members had been notified in an appropriate fashion, and had the information
3 not been hidden from them, they could have taken precautions to safeguard and protect their
4 PII/PHI, medical information, and identities.

5
6 157. Defendant’s above-described wrongful actions, inaction, omissions, want of
7 ordinary care, misrepresentations, practices, and non-disclosures also constitute “unfair or
8 deceptive acts or practices” in violation of the CPA in that Defendant’s wrongful conduct is
9 substantially injurious to other persons, had the capacity to injure other persons, and has the
10 capacity to injure other persons.

11
12 158. The gravity of Defendant’s wrongful conduct outweighs any alleged benefits
13 attributable to such conduct. There were reasonably available alternatives to further Defendant’s
14 legitimate business interests other than engaging in the above-described wrongful conduct.

15
16 159. As a direct and proximate result of Defendant’s above-described wrongful actions,
17 inaction, omissions, and want of ordinary care that directly and proximately caused the Data
18 Breach and their violations of the CPA, Plaintiff and Class Members have suffered, and will
19 continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*,
20 (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and
21 medical fraud—risks justifying expenditures for protective and remedial services for which he or
22 she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of his or
23 her PII/PHI; (5) deprivation of the value of his or her PII/PHI, for which there is a well-established
24 national and international market; and/or (v) the financial and temporal cost of monitoring credit,
25 monitoring financial accounts, and mitigating damages.

1 165. Defendant had, and continue to have, a duty to timely disclose that Plaintiff’s and
2 Class Members’ Private Information within their possession was compromised and precisely the
3 type(s) of information that were compromised.

4 166. Defendant had a duty to have procedures in place to detect and prevent the loss or
5 unauthorized dissemination of Plaintiff’s and Class Members’ Private Information.

6 167. Defendant owed a duty of care to Plaintiff and Class Members to provide data
7 security consistent with industry standards, applicable standards of care from statutory authority
8 like HIPPA and Section 5 of the FTC Act, and other requirements discussed herein, and to ensure
9 that their systems and networks, and the personnel responsible for them, adequately protected the
10 Private Information.
11

12 168. Defendant’s duty of care to use reasonable security measures arose as a result of
13 the special relationship that existed between Defendant and its patients, which is recognized by
14 laws and regulations including but not limited to HIPAA, as well as common law. Defendant was
15 in a position to ensure that its systems were sufficient to protect against the foreseeable risk of
16 harm to Class Members from a data breach.
17

18 169. Defendant’s duty to use reasonable security measures under HIPAA required
19 Defendant to “reasonably protect” confidential data from “any intentional or unintentional use or
20 disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to
21 protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1). Some or all of the
22 medical information at issue in this case constitutes “protected health information” within the
23 meaning of HIPAA.
24

25 170. In addition, Defendant had a duty to employ reasonable security measures under
26

1 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . .
2 practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair
3 practice of failing to use reasonable measures to protect confidential data.

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

7 172. Defendant systematically failed to provide adequate security for data in its
8 possession.

9 173. The specific negligent acts and omissions committed by Defendant include, but are
10 not limited to, the following:

- 11
- 12 a. Upon information and belief, mishandling emails, so as to allow for
 - 13 unauthorized person(s) to access Plaintiff’s and Class Members’ Private
 - 14 Information;
 - 15 b. Failing to adopt, implement, and maintain adequate security measures to
 - 16 safeguard Class Members’ Private Information;
 - 17 c. Failing to adequately monitor the security of their networks and systems;
 - 18 d. Failure to periodically ensure that their computer systems and networks had
 - 19 plans in place to maintain reasonable data security safeguards.
 - 20
 - 21

22 174. Defendant, through its actions and/or omissions, unlawfully breached their duty to
23 Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding
24 Plaintiff’s and Class Members’ Private Information within Defendant’s possession.

25 175. Defendant, through its actions and/or omissions, unlawfully breached their duty to
26

1 Plaintiff and Class members by failing to have appropriate procedures in place to detect and
2 prevent dissemination of Plaintiff's and Class Members' Private Information.

3 176. Defendant, through its actions and/or omissions, unlawfully breached their duty to
4 timely disclose to Plaintiff and Class Members that the Private Information within Defendant's
5 possession might have been compromised and precisely the type of information compromised.
6

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

11 178. It was foreseeable that the failure to adequately safeguard Plaintiff and Class
12 Members' Private Information would result in injuries to Plaintiff and Class Members.
13

14 179. Defendant's breach of duties owed to Plaintiff and Class Members caused
15 Plaintiff's and Class Members' Private Information to be compromised.

16 180. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members
17 regarding what type of Private Information has been compromised, Plaintiff and Class Members
18 are unable to take the necessary precautions to mitigate damages by preventing future fraud.

19 181. Defendant's breaches of duty caused Plaintiff and Class Members to suffer from
20 identity theft, loss of time and money to monitor their finances for fraud, and loss of control over
21 their Private Information.
22

23 182. As a result of Defendant's negligence and breach of duties, Plaintiff and Class
24 Members are in danger of imminent harm in that their Private Information, which is still in the
25 possession of third parties, will be used for fraudulent purposes.
26

1 183. Plaintiff seeks the award of actual damages on behalf of the Class.

2 184. In failing to secure Plaintiff's and Class Members' Private Information and
3 promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice,
4 in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiff's and
5 Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive
6 damages on behalf of herself and the Class.
7

8 185. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1)
9 compelling Defendant to institute appropriate data collection and safeguarding methods and
10 policies with regard to patient information; and (2) compelling Defendant to provide detailed and
11 specific disclosure of what types of Private Information have been compromised as a result of the
12 data breach.
13

14 **FOURTH COUNT**
15 **Breach of Express Contract**
(On Behalf of Plaintiff and All Class Members)

16 186. The preceding factual statements and allegations are incorporated by reference.

17 187. Plaintiff and Class Members entered into express contracts with Defendant that
18 include Defendant's promise provide medical care and treatment, and the promise to protect
19 nonpublic personal information given to Defendant or that Defendant gathers on its own from
20 disclosure. The express contract is embodied in the Privacy Notice and the Signed
21 Acknowledgment, and (upon information and belief) in other documents.
22

23 188. Plaintiff and Class Members performed their obligations under the contract when
24 they paid for their health care services and gave Defendant their Private Information (which also
25 constitutes good and valuable consideration).
26

1 189. Defendant should have used some of Plaintiff's payments (or payments made on
2 his behalf) to institute adequate protection of Plaintiff's Private Information, but Defendant did
3 not.

4 190. As a result, Defendant exposed Plaintiff's Private Information during the Data
5 Breach.

6 191. Plaintiff and Class Members thus paid Defendant for promised data security
7 protections that they never received.

8 192. Had Plaintiff known of Defendant's substandard methods of protecting her Private
9 Information, he would have sought medical care elsewhere.

10 193. Defendant breached its contractual obligation to protect the nonpublic personal
11 information Defendant gathered when the information was accessed by unauthorized personnel as
12 part of the Data Breach.

13 194. As a direct and proximate result of the breach, Plaintiff and Class Members have
14 been harmed and have suffered, and will continue to suffer, damages and injuries, and are entitled
15 to actual, compensatory, and nominal damages.

16
17
18 **FIFTH COUNT**
19 **Breach of Implied Contract**
20 **(On Behalf of Plaintiff and All Class Members)**

21 195. The preceding factual statements and allegations are incorporated by reference.

22 196. Defendant provided Plaintiff and Class Members with an implied contract to protect
23 and keep Defendant's patients' private, nonpublic personal, financial and health information when
24 they gathered the information from each of their patients.

25 197. When Plaintiff and Class Members provided their Private Information to Defendant
26

1 in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant
2 to which Defendant agreed to reasonably protect such information.

3 198. Defendant's agreement to reasonably protect such information included
4 compliance with healthcare industry data security standards, and with applicable data security
5 standards that govern healthcare entities like Defendant, including HIPAA.
6

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

10 200. In entering into such implied contracts, Plaintiff and Class Members reasonably
11 believed and expected that Defendant's data security practices complied with relevant laws and
12 regulations, including HIPAA, and were consistent with industry standards.
13

14 201. HIPAA requires covered entities like Defendant to protect against reasonably
15 anticipated threats to the security of sensitive patient health information.

16 202. HIPAA covered entities must implement safeguards to ensure the confidentiality,
17 integrity, and availability of PHI. Safeguards must include physical, technical, and administrative
18 components.
19

20 203. Healthcare industry standards for data security include several best practices that
21 have been identified that a minimum should be implemented by healthcare providers like
22 Defendant. These include, but are not limited to: educating all employees; strong passwords; multi-
23 layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data
24 unreadable without a key; multi-factor authentication; backup data, and; limiting which employees
25 can access sensitive data.
26

1 204. Other best cybersecurity practices that are standard in the healthcare industry
2 include installing appropriate malware detection software; monitoring and limiting the network
3 ports; protecting web browsers and email management systems; setting up network systems such
4 as firewalls, switches and routers; monitoring and protection of physical security systems;
5 protection against any possible communication system; training staff regarding critical points.
6

7 205. Class Members who paid money to Defendant, or who had money paid on their
8 behalf to Defendant, reasonably believed and expected that Defendant would use part of those
9 funds to obtain adequate data security that complied with healthcare industry data security
10 standards and applicable regulations like HIPAA. Defendant failed to do so.

11 206. Plaintiff and Class Members would not have provided their personal, financial or
12 health information to Defendant, but for Defendant's implied promises to safeguard and protect
13 Defendant's patients' private personal, financial, and health information.
14

15 207. Plaintiff and Class Members performed their obligations under the implied contract
16 when they provided their private personal, financial, and health information as a patient and when
17 they paid for the services provided by Defendant.

18 208. Defendant breached the implied contracts with Plaintiff and Class Members by
19 failing to protect and keep private the nonpublic personal, financial, and health information
20 provided to them about Plaintiff and Class Members.
21

22 209. As a direct and proximate result of Defendant's breach of their implied contracts,
23 Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer,
24 damages and injuries.
25
26

SIXTH COUNT

Breach of Confidence

(On Behalf of Plaintiff and All Class Members)

1
2
3 210. The preceding factual statements and allegations are incorporated by reference.

4 211. At all times during Plaintiff's and the Class's interactions with Defendant,
5 Defendant were fully aware of the confidential and sensitive nature of Plaintiff's and the Class's
6 PII and PHI that Plaintiffs and the Class provided to Defendant.

7 212. As alleged herein and above, Defendant's relationship with Plaintiff and the Class
8 was governed by terms and expectations that Plaintiff's and the Class's PII and PHI would be
9 collected, stored, and protected in confidence, and would not be disclosed to unauthorized third
10 parties.

11
12 213. Plaintiff and the Class provided their PII and PHI to Defendant with the explicit
13 and implicit understandings that Defendant would protect and not permit the PII and PHI to be
14 disseminated to any unauthorized third parties.

15 214. Plaintiff and the Class also provided their PII and PHI to Defendant with the explicit
16 and implicit understandings that Defendant would take precautions to protect that PII and PHI
17 from unauthorized disclosure.

18 215. Defendant voluntarily received in confidence Plaintiff's and the Class's PII and
19 PHI with the understanding that PII and PHI would not be disclosed or disseminated to the public
20 or any unauthorized third parties.

21 216. Due to Defendant's failure to prevent and avoid the Data Breach from occurring,
22 Plaintiff's and the Class's PII and PHI was disclosed and misappropriated to unauthorized third
23 parties beyond Plaintiff's and the Class's confidence, and without their express permission.

24 217. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff
25
26

1 and the Class have suffered damages.

2 218. But for Defendant’s disclosure of Plaintiff’s and the Class’s PII and PHI in violation
3 of the parties’ understanding of confidence, their PII and PHI would not have been compromised,
4 stolen, viewed, accessed, and used by unauthorized third parties. Defendant’s Data Breach was the
5 direct and legal cause of the theft of Plaintiff’s and the Class’s PII and PHI as well as the resulting
6 damages.
7

8 219. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable
9 result of Defendant’s unauthorized disclosure of Plaintiff’s and the Class’s PII and PHI. Defendant
10 knew or should have known its methods of accepting and securing Plaintiff’s and the Class’s PII
11 and PHI was inadequate as it relates to, at the very least, securing servers and other equipment
12 containing Plaintiff’s and the Class’s PII and PHI.
13

14 220. As a direct and proximate result of Defendant’s breach of its confidence with
15 Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but
16 not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used;
17 (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses
18 associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or
19 unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended
20 and the loss of productivity addressing and attempting to mitigate the actual present and future
21 consequences of the Data Breach, including but not limited to efforts spent researching how to
22 prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with
23 placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in
24 Defendant’s possession and is subject to further unauthorized disclosures so long as Defendant
25
26

1 fails to undertake appropriate and adequate measures to protect the PII and PHI of current and
2 former patients and their beneficiaries and dependents; and (viii) present and future costs in terms
3 of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact
4 of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of
5 Plaintiff and the Class.
6

7 221. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff
8 and the Class have suffered and will continue to suffer other forms of injury and/or harm,
9 including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and
10 non-economic losses.

11 **PRAYER FOR RELIEF**

12 WHEREFORE, Plaintiff prays for judgment as follows:

13 A. For an Order certifying this action as a class action and appointing Plaintiff and her
14 Counsel to represent the Class;
15

16 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct
17 complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members'
18 Private Information, and from refusing to issue prompt, complete and accurate disclosures to
19 Plaintiff and Class Members;
20

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

24 D. For equitable relief requiring restitution and disgorgement of the revenues
25 wrongfully retained as a result of Defendant's wrongful conduct;
26

1 E. Ordering Defendant to pay for not less than three years of credit monitoring services
2 for Plaintiff and the Class;

3 F. Ordering Defendant to disseminate individualized notice of the Data Breach to all
4 Class Members;

5 G. For an award of actual damages, compensatory damages, statutory damages, and
6 statutory penalties, in an amount to be determined, as allowable by law;

7 H. For an award of punitive damages, as allowable by law;

8 I. For an award of attorneys' fees and costs, and any other expense, including expert
9 witness fees;

10 J. Pre- and post-judgment interest on any amounts awarded; and

11 K. Such other and further relief as this court may deem just and proper.
12
13
14

15 RESPECTFULLY SUBMITTED this 11th day of November, 2020.

16 FRANK FREED SUBIT & THOMAS LLP

17
18 By: /s/ Michael C. Subit
19 Michael C. Subit, WSBA No. 29189
20 705 Second Avenue, Suite 1200
21 Seattle, Washington 98104-1798
22 (206) 682-6711 (phone)
23 (206) 682-0401 (fax)
24 msubit@frankfreed.com

25 (Local Counsel)
26

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

MASON LIETZ & KLINGER LLP

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

MASON LIETZ & KLINGER LLP

Gary M. Klinger (*pro hac vice forthcoming*)
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (312) 283-3814
Fax: (773) 496-8617
gklinger@masonllp.com

(Lead Counsel)

*Attorneys for Plaintiff and
the Proposed Classes*