

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

LYNETTE WALIANY, on behalf of herself
and all others similarly situated,

Plaintiff,

v.

SEA MAR COMMUNITY HEALTH
CENTERS,

Defendant.

Case No.

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

(Clerk’s Action Required)

King County Superior Court
Case No. 21-2-16813-9 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, Case No. 21-2-16813-9 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, *Lynette Waliany, on behalf of herself and all*

1 *others similarly situated v. Sea Mar Community Health Centers*, was filed in King County
2 Superior Court, State of Washington, on December 23, 2021. A true and correct copy of the
3 Class Action Complaint filed in King County Superior Court Case No: 21-2-16813-9 SEA is
4 attached as **Exhibit A**. This is a civil action arising out of alleged violations of (1) RCW
5 19.255.010, Washington Data Breach Disclosure Law, and (2) RCW 19.86.101 Washington
6 Consumer Protection Act; as well as allegations of (3) negligence, (4) breach of implied contract,
7 (5) breach of good faith and fair dealing, and (6) invasion of privacy-tort of public disclosure,
8 with claims made by Plaintiffs for compensatory, exemplary, punitive, restitution, and statutory
9 damages; attorney fees and costs; pre- and post-judgment interest; and injunctive and equitable
10 relief.

11 **II. GROUNDS FOR REMOVAL**

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

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

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

22 **B. The Federal Tort Claims Act, 28 U.S.C. 1346(b) Applies to Plaintiffs’ 23 Claims.**

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

27 Subject to the provisions of chapter 171 of this title, the district

1 courts . . . shall have exclusive jurisdiction of civil actions against
2 the United States . . . for injury or loss of property, or personal
3 injury or death caused by the negligent or wrongful act or omission
4 of any employee of the Government while acting within the scope
5 of his office or employment, under circumstances where the United
6 States, if a private person, would be liable to the claimant in
7 accordance with the law of the place where the act or omission
8 occurred.

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

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

12 The Public Health Service Act provides liability protection to Public Health Service
13 (“PHS”) employees like Sea Mar under the Federal Tort Claims Act, 28 U.S.C. §§ 1346(b). Sea
14 Mar is a PHS employee under the Federally Supported Health Centers Assistance Act, 42 U.S.C.
15 §§ 233(g)-(n). The *exclusive* remedy for damage for personal injury “resulting from the
16 performance of medical, surgical, dental, or *related functions*, . . . by any commissioned . . .
17 employee of the Public Health Service while acting within the scope of his office or
18 employment” is *against the United States*. 42 U.S.C. § 233(a). Plaintiffs allege they suffered
19 personal injuries, including anxiety and emotional distress, as a result of a data breach incident in
20 the Sea Mar environment. The Federally Supported Health Centers Assistance Act (42 U.S.C. §
21 233(a)) provides absolute immunity for PHS employees acting within the scope of their
22 employment. *Hui v. Castaneda*, 559 U.S. 799, 806 (2010).

23 **D. Sea Mar’s Conduct Was Function Required and Related to the Provision 24 of Medical Care.**

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

1 the “related functions” to medical care—creating and maintaining medical, financial and other
2 personal records of patients and their guarantors. Sea Mar qualifies for immunity, and in an
3 FTCA suit, a plaintiff’s exclusive remedy is to proceed in an action against the United States in
4 district court.

5 **III. TIME FOR REMOVAL**

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

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

16 **IV. REQUIRED DOCUMENTS**

17 Defendant Sea Mar will promptly give written notice to all adverse parties. 28 USC §
18 1446(d).

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

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

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

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 this 16th day of February, 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 certify that on February 16, 2022, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to all attorneys of record and provide service via electronic mail to:

Samuel J. Strauss, WSBA #46971 TURKE & STRAUSS LLP 936 North 34th Street, Suite 300 Seattle, Washington 98103-8869 (608) 237-1775 <i>Attorney 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 (608) 509-4423 <input checked="" type="checkbox"/> via CM/ECF <input checked="" type="checkbox"/> via E-mail: sam@turkestrauss.com
Walter Smith, WSBA #46695 SMITH & DIETRICH LAW OFFICES PLLC 3905 Martin Way E., Suite F Olympia, WA 98506 (360) 915-6952 <i>Attorney 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: walter@smithdietrich.com
Nicholas W. Brown Kristen R. Vogel, NY No. 5195664 Assistant United States Attorney Western District of Washington 700 Stewart Street, Suite 5220 Seattle, Washington 98101-1271 (206) 553-7970 / (206) 553-4067 Fax <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/ Tami L. Foster

Tami L. Foster, Legal Assistant
Tami.Foster@lewisbrisbois.com

0S00
GEGFÄÖÖÄGHÄFKHÄJT
SÖÖÄUWÄVY
ÜWÜÖÜWÜÄÜWÜVÄÖSÖS
ÖÖSÖÖ
ÖÜÖÄKÖFÖFÏFHEÄÜÖE

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

LYNETTE WALIANY, on behalf of herself
and all others similarly situated,

Plaintiff,

v.

SEA MAR COMMUNITY HEALTH
CENTERS,

Defendant.

NO.

CLASS ACTION COMPLAINT

For:

1. Negligence;
2. Breach of Implied Contract;
3. Violation of the Washington Consumer Protection Act, RCW § 19.86, *et seq.*;
4. Violation of the Washington Data Breach Disclosure Law RCW § 19.255.010; and
5. Unjust Enrichment.

Plaintiff, Lynette Waliany (“Ms. Waliany” or “Plaintiff”), by counsel, brings this Class Action Complaint against the Defendant, Sea Mar Community Health Centers (“Sea Mar” or “Defendant”), alleging as follows:

I. INTRODUCTION

1.1 Sea Mar, a multimillion-dollar medical service provider headquartered in Washington state, lost control over its patients’ highly sensitive medical and personal data in a data breach by cybercriminals that spanned from approximately December 2020 to March 2021 (“Data Breach”). The cybercriminals copied patient data and then auctioned it for sale online to the highest bidders. The stolen information included highly sensitive personally identifying information (“PII”) and personal health information (“PHI”). Cybercriminals could pilfer

1 patients' PII and PHI because Sea Mar did not adequately maintain, protect, and secure the
2 information, leaving it an unguarded target for theft and misuse. On information and belief, Sea
3 Mar knew or had reason to know that patients' PII and PHI was for sale online but never
4 informed its patients of that fact. Ms. Waliany was a victim of the Sea Mar Data Breach and
5 brings this Class Action on behalf of all patients harmed by Sea Mar's conduct.

6 1.2 On June 24, 2021, cybercriminals advertised the Sea Mar patient data for sale
7 online through a website managed by cybercriminals under the organization name "Marketo."
8 Marketo's cybercriminals advertised that they had over three terabytes of patient data for sale,
9 offering a sample of the information in a downloadable "evidence pack." On information and
10 belief, Marketo's "evidence pack" had photos of patients, including pediatric patients, each with
11 the patient's name, date of birth, date of photo, and insurance information related to their
12 treatment.

13 1.3 Sea Mar learned about this disturbing breach the same day, June 24, 2021. But
14 Sea Mar did not immediately inform its patients about the breach as required by Washington law.
15 Instead, Sea Mar waited over three months before it informed patients that it had lost control
16 over their highly sensitive PII and PHI.

17 1.4 Sea Mar internally investigated the Data Breach, which revealed that
18 "unauthorized" bad actors had in fact breached its systems, copying patient data, including data
19 from December 2020 through March 2021. According to Sea Mar, the stolen PII and PHI
20 included "patient names, addresses, Social Security numbers, dates of birth, client identification
21 numbers, medical/dental/orthodontic diagnostic and treatment information, medical/vision/dental
22 insurance information, claims information, and/or images associated with dental treatment."

23 1.5 On information and belief, by July 2021, Marketo's auction for the PII and PHI
24 had purportedly garnered over 200 bids for patients' highly sensitive data.

25 1.6 On August 31, 2021, Sea Mar concluded its internal investigation, but it still did
26 not immediately inform patients of the Data Breach. Instead, Sea Mar waited until October 29,
2021, to announce the breach by notice to patients ("Breach Notice").

1 1.7 Sea Mar’s Breach Notice hid the nature of the Data Breach and the risk it posed to
2 patients. The Breach Notice informed patients that Sea Mar was subject to a breach that led to
3 Sea Mar losing control over patients’ PII and PHI. But the Breach Notice omitted that
4 cybercriminals had advertised their PII and PHI for sale at an online auction that had received
5 over 200 bids. Instead, Sea Mar claimed it was “not aware of any evidence of the misuse of any
6 information potentially involved in this incident.”

7 1.8 Sea Mar’s failure to protect patients’ PII and PHI and failure to inform patients
8 promptly and fully about the Data Breach violates Washington law and harms hundreds of
9 thousands of patients, causing Ms. Walianny to seek relief on a class wide basis.

10 **II. PARTIES**

11 2.1 Plaintiff, Ms. Walianny, is an individual residing in Puyallup, Washington. Since
12 2015, Ms. Walianny has used Sea Mar’s healthcare and dental services and continues to use them
13 through the present. Ms. Walianny is a victim of the Sea Mar Data Breach and has received Sea
14 Mar’s Breach Notice.

15 2.2 Sea Mar is a medical and dental services provider headquartered in Seattle,
16 Washington. Sea Mar has offices around Washington state and provides services to individuals
17 residing inside and outside Washington state.

18 **III. JURISDICTION AND VENUE**

19 3.1 Jurisdiction is proper in this Court under RCW § 2.08.010 since the amount in
20 controversy exceeds the jurisdictional threshold of the Superior Court.

21 3.2 This Court has personal jurisdiction over Sea Mar because it is incorporated under
22 the laws of Washington, and its principal place of business is located in Washington state.

23 3.3 Venue is proper in this Court under RCW § 4.12.020(3) because King County is
24 where the causes of action resulting from the Data Breach arose.

25 //
26

IV. FACTUAL ALLEGATIONS

A. Sea Mar

4.1 Sea Mar is a medical and dental services provider headquartered in Washington state, providing medical, dental, behavioral health, pharmaceutical, long-term care, and substance abuse services in 13 Washington counties.

4.2 From April 2019 to March 2020, Sea Mar reportedly saw around 304,000 patients in over 1.6 million patient encounters.¹ In that time, Sea Mar also reportedly received \$383,599,899.00 in revenue.

4.3 Sea Mar promises to safeguard patients’ PII and PHI as part of its services, providing patients its Notice of Privacy Practices.

4.4 Sea Mar’s Notice of Privacy Practices recognizes Sea Mar’s duty to secure and maintain patient PII and PHI:²

Notice Privacy Practices



This notice describes how medical information about you may be used and disclosed, and how you can get access to this information. Please review it carefully.

Sea Mar Community Health Centers respects your privacy. We understand that your personal health information is very sensitive. We will not disclose your information to others unless you tell us to do so, or unless the law authorizes or requires us to do so.

The law protects the privacy of the health information we create and obtain in providing health care and services to you. For example, your protected health information includes your symptoms, test results, diagnoses, treatment, health information from other providers, and billing and payment information relating to these services. Federal and state law allows us to use and disclose your protected health information for purposes of treatment and health care operations to others. State law requires us to get your authorization to disclose this information for payment purposes.

4.5 The PII and PHI Sea Mar collects includes patient names, addresses, Social Security numbers, dates of birth, client identification numbers, medical/dental/orthodontic

¹ See Sea Mar’s Report to the Community 2020, <https://www.seamar.org/seamar-downloads/Annual-Report2020.pdf> (last visited Dec. 21, 2021).

² See Sea Mar’s Notice of Privacy Practices, <https://seamar.org/notice.html> (last visited Dec. 21, 2021).

1 diagnostic and treatment information, medical/vision/dental insurance information, claims
2 information, or images associated with dental treatment.

3 **B. Sea Mar fails to safeguard patients' PII and PHI**

4 4.6 Ms. Waliandy and the proposed Class are current and former Sea Mar patients.

5 4.7 As a condition to providing treatment, Sea Mar required Ms. Waliandy and the
6 proposed Class to provide PII and PHI.

7 4.8 Sea Mar then collected and maintained patients' PII and PHI in its computer
8 systems.

9 4.9 In collecting and storing patients' PII and PHI, Sea Mar represented to patients
10 that Sea Mar would protect and maintain their data according to state and federal law.

11 4.10 Ms. Waliandy and the proposed Class relied on Sea Mar's representations in
12 agreeing to provide their PII and PHI.

13 4.11 On information and belief, on June 24, 2021, cybercriminals on the online stolen
14 data marketplace, "Marketo," advertised that they had over three terabytes of Sea Mar patient
15 data available for sale.

16 4.12 Cybercriminals had accessed Sea Mar's systems at some time before advertising
17 the data for sale on Marketo. The Marketo advertisement included a description of the data and
18 Sea Mar's failure to protect patient data.³

19
20
21
22
23
24
25
26

³ See *WA: Sea Mar Community Health Centers discloses breach that began last year*
<https://www.databreaches.net/wa-sea-mar-community-health-centers-discloses-breach-that-began-last-year/> (last
visited Dec. 21, 2021).

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17

Sea Mar Community Health Centers
Sea Mar Community Health Centers | site: seamar.org

3 TB Download evidence pack

Sea Mar Community Health Centers is a community-based organization committed to providing health, human, housing, educational and cultural services to diverse communities, specializing in service to Latinos in Washington state. Your attempts at tolerance do not make up for other sins. You serve all persons without regard to race, ethnicity, immigration status, gender, or sexual orientation, and regardless of ability to pay for services. But you decided to forget without remorse about the quality of the provided services and the clients' right to confidentiality. Customers do not come to you for services so that photos of their sick, crooked teeth are publicly available. Their beautiful, contended smiles are just a part of the interesting data leaked online. Personal letters (emails), photos and contacts of clients, photos of agreements - here is a worthy reason to smile for your customers, partners and competitors, because your accent on tolerance led to poor-quality services and and allowed hacking. Say "cheese" and smile with your beautiful teeth.

Washington health medicine Seamar

Bids counter: 197 (+1 for today)

VIP

18 4.13 On information and belief, Marketo also included a downloadable “evidence
19 pack,” which included sample files from the Data Breach. According to an investigation by
20 Databreaches.net, the evidence pack “contained a few photos of identified pediatric dental
21 patients. Each one held a sign with their name, date of birth, and date of photo. There were also
22 a few insurance-related forms with patient information.”⁴

23 4.14 Marketo included a “Bids counter” which purportedly tracked how many bids the
24 patients’ PII and PHI had received.

25 4.15 On information and belief, as of July 2021, Sea Mar’s lost data had garnered over
26 200 bids on Marketo.

⁴ *Id.*

1 **C. Sea Mar learns of the Data Breach and Fails to Immediately Disclose the**
2 **Breach to Plaintiff and the Proposed Class**

3 4.16 On or about June 24, 2021, Sea Mar learned that its data systems had been
4 breached, the same day Marketo advertised patients’ PII and PHI for sale by auction.

5 4.17 On information and belief, Sea Mar learned about the Data Breach from a third-
6 party that alerted it to Marketo’s online auction.

7 4.18 Sea Mar did not immediately alert patients or the public generally that its patients’
8 data had been stolen.

9 4.19 Instead, Sea Mar chose to internally investigate the Data Breach for months while
10 patients’ highly sensitive PII and PHI garnered bids online.

11 4.20 According to Sea Mar, its internal investigation revealed that it lost control over
12 patients’ PII and PHI, including photos from patient procedures: “The following personal and
13 protected health information may have been involved in the incident: Name, address, Social
14 Security number, date of birth, client identification number, medical / vision / dental /
15 orthodontic diagnostic and treatment information, medical / vision / dental insurance
16 information, claims information, and / or images associated with dental treatment.”

17 4.21 Sea Mar also purportedly learned that “additional data may have been removed
18 from its digital environment between December 2020 and March 2021.”

19 4.22 On August 30, 2021, Sea Mar completed its internal investigation. Even so, Sea
20 Mar *still* did not inform patients or the public generally about the Data Breach for another two
21 months.

22 4.23 On October 29, 2021—three months after learning about the Data Breach—Sea
23 Mar finally sent the Breach Notice to 628,569 potentially affected patients. A true and accurate
24 copy of a sample Breach Notice is attached to this Complaint as Exhibit A.

25 4.24 Sea Mar’s Breach Notice described the Data Breach vaguely without explaining
26 who breached Sea Mar’s systems, how the breach occurred, or how Sea Mar learned of the

1 breach: “On June 24, 2021, Sea Mar *was informed* that certain data belonging thereto had been
2 copied from the Sea Mar digital environment.” (emphasis added).

3 4.25 The Breach Notice excluded critical information; namely, that patients’ PII and
4 PHI had been advertised for sale by cybercriminals at an online auction.

5 4.26 Instead, Sea Mar’s Breach Notice hid the disturbing nature of the Data Breach,
6 misrepresenting that Sea Mar “ha[d] no evidence that any potentially affected information has
7 been misused.”

8 4.27 The Breach Notice also did not clarify how many times hackers breached its
9 systems, when they breached Sea Mar’s systems, exactly what they took, and how Sea Mar
10 changed its security protocols to prevent future breaches.

11 4.28 On October 29, 2021, Sea Mar disclosed the Data Breach to the Washington
12 Attorney General’s Office by letter from Sea Mar’s attorneys.

13 4.29 On November 5, 2021, Sea Mar also disclosed the Data Breach to the Maine
14 Attorney General’s Office because it determined around 58 Maine residents were affected by the
15 Data Breach.

16 4.30 Neither notice to the Washington or Maine Attorneys General offices included
17 that patient’s PII and PHI had been advertised for sale online by cybercriminals.

18 4.31 On information and belief, Sea Mar failed to adequately train its employees on
19 reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose
20 control over patients’ PII and PHI. Sea Mar’s negligence is evidenced by its failure to recognize
21 the Data Breach until Marketo listed patient data online for sale, meaning Sea Mar had no
22 effective means to detect and prevent attempted data breaches. Further, the Breach Notice makes
23 clear that Sea Mar cannot even determine the full scope of the Data Breach, as it has been unable
24 to determine exactly what information was stolen and when.

25 **D. Plaintiff’s Experience**

26 4.32 Ms. Walianny has been a patient at Sea Mar from 2015 through the present.

1 4.33 As a condition of receiving treatment, Sea Mar requires Ms. Walianny to provide
2 her PII and PHI.

3 4.34 Since becoming a Sea Mar patient, Ms. Walianny has provided Sea Mar her PII
4 and PHI to purchase Sea Mar's treatment services.

5 4.35 Following the Data Breach in June 2021, Ms. Walianny became aware that her PII
6 and PHI were compromised by the Data Breach.

7 4.36 In response, Ms. Walianny has spent considerable time and effort monitoring her
8 accounts to protect herself from additional identity theft. Ms. Walianny fears for her personal
9 financial security and uncertainty over what medical information was revealed in the Data
10 Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the
11 Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the
12 sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

13 4.37 Further, Ms. Walianny is unsure what has happened to her PII and PHI as Sea Mar
14 has been unwilling to disclose the true nature of the Data Breach or what measures it has taken to
15 safeguard her PII and PHI in the future.

16 **E. Ms. Walianny and the Proposed Class Face Significant Risk of Identity Theft**

17
18 4.38 Ms. Walianny and members of the proposed class have suffered injury from the
19 misuse of their PII and PHI that can be directly traced to Sea Mar.

20 4.39 The ramifications of Sea Mar's failure to keep Plaintiff's and the Class's PII and
21 PHI secure are severe. Identity theft occurs when someone uses another's personal and financial
22 information such as that person's name, account number, Social Security number, driver's
23 license number, date of birth, or other information, without permission, to commit fraud or other
24 crimes.

25 4.40 According to experts, one out of four data breach notification recipients become a
26 victim of identity fraud.

1 4.41 Because Sea Mar failed to prevent the Data Breach, Ms. Waliany and the
2 proposed Class have suffered and will continue to suffer damages, including monetary losses,
3 lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of
4 suffering:

- 5 a. The loss of the opportunity to control how their PII and PHI are used;
- 6 b. The diminution in value of their PII and PHI;
- 7 c. The compromise and continuing publication of their PII and PHI;
- 8 d. Out-of-pocket costs associated with the prevention, detection, recovery, and
9 remediation from identity theft or fraud;
- 10 e. Lost opportunity costs and lost wages associated with the time and effort
11 expended addressing and trying to mitigate the actual and future consequences of
12 the Data Breach, including, but not limited to, efforts spent researching how to
13 prevent, detect, contest, and recover from identity theft and fraud;
- 14 f. Delay in receipt of tax refund monies;
- 15 g. Unauthorized use of stolen PII and PHI; and
- 16 h. The continued risk to their PII and PHI, which remains in the possession of Sea
17 Mar and is subject to further breaches so long as Sea Mar fails to undertake the
18 appropriate measures to protect the PII and PHI in their possession.

19 4.42 Stolen PII and PHI is one of the most valuable commodities on the criminal
20 information black market. According to Experian, a credit-monitoring service, an individual's
21 stolen PHI can be worth up to \$1,000.00 depending on the type of information obtained.

22 4.43 The value of Plaintiff's and the proposed Class's PII and PHI on the black market
23 is considerable. Stolen PII and PHI trades on the black market for years, and criminals often post
24 stolen private information openly on various "dark web" internet websites, like Marketo, making
25 the information publicly available, for a fee.

26 4.44 It can take victims years to spot identity or PII and PHI theft, giving criminals
time to sell that information for cash.

1 4.45 One such example of criminals using PII and PHI for profit is the development of
2 “Fullz” packages.

3 4.46 Cybercriminals can cross-reference two sources of PII and PHI to marry
4 unregulated data available elsewhere to criminally stolen data with an astonishingly complete
5 scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are
6 known as “Fullz” packages.

7 4.47 The development of “Fullz” packages means that stolen PII and PHI from the
8 Data Breach can easily be used to link and identify it to Plaintiff’s and the proposed Class’s
9 phone numbers, email addresses, and other unregulated sources and identifiers. In other words,
10 even if certain information such as emails, phone numbers, or credit card numbers may not be
11 included in the PII and PHI stolen by the cybercriminals in the Data Breach, criminals can easily
12 create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such
13 as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff
14 and members of the proposed Class, and it is reasonable for any trier of fact, including this Court
15 or a jury, to find that Plaintiff’s and other members of the proposed Class’ stolen PII and PHI is
16 being misused, and that such misuse is fairly traceable to the Data Breach.

17 4.48 According to the FBI’s Internet Crime Complaint Center (IC3) 2019 Internet
18 Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar
19 losses that year, leading to more than \$3.5 billion in losses to individuals and business victims.

20 4.49 Further, according to the same report, “rapid reporting can help law enforcement
21 stop fraudulent transactions before a victim loses the money for good.” Sea Mar did not rapidly
22 report to Plaintiff, the Class, or the Washington Attorney General that patient PII and PHI had
23 been stolen.

24 4.50 Victims of identity theft also often suffer embarrassment, blackmail, or
25 harassment in person or online, and experience financial losses resulting from fraudulently
26 opened accounts or misuse of existing accounts.

1 4.51 Along with out-of-pocket expenses that can exceed thousands of dollars for the
2 victim of new account identity theft, and the emotional toll identity theft can take, some victims
3 must spend a considerable time repairing the damage caused by the theft of their PHI. Victims of
4 new account identity theft will likely have to spend time correcting fraudulent information in
5 their credit reports and continually monitor their reports for future inaccuracies, close existing
6 bank/credit accounts, open new ones, and dispute charges with creditors.

7 4.52 Further complicating the issues faced by victims of identity theft, data thieves
8 may wait years before trying to use the stolen PII and PHI. To protect themselves, Ms. Waliany
9 and the Class will need to remain vigilant against unauthorized data use for years or even
10 decades to come.

11 4.53 The Federal Trade Commission (“FTC”) has also recognized that consumer data
12 is a new and valuable form of currency. In an FTC roundtable presentation, former
13 Commissioner, Pamela Jones Harbour, stated that “most consumers cannot begin to comprehend
14 the types and amount of information collected by businesses, or why their information may be
15 commercially valuable. Data is currency.”

16 4.54 The FTC has also issued several guidelines for businesses that highlight
17 reasonable data security practices. The FTC has noted the need to factor data security into all
18 business decision-making. According to the FTC, data security requires: (1) encrypting
19 information stored on computer networks; (2) retaining payment card information only as long as
20 necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting
21 administrative access to business systems; (5) using industry-tested and accepted methods for
22 securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying
23 that privacy and security features function properly; (8) testing for common vulnerabilities; and
24 (9) updating and patching third-party software.

25 4.55 According to the FTC, unauthorized PHI disclosures are extremely damaging to
26 consumers’ finances, credit history, and reputation, and can take time, money, and patience to
resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to

1 protect against unauthorized access to confidential consumer data as an unfair act or practice
2 prohibited by Section 5(a) of the FTC Act.

3 4.56 To that end, the FTC has issued orders against businesses that failed to employ
4 reasonable measures to secure sensitive payment card data. *See In the matter of Lookout*
5 *Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) (“[Defendant] allowed users to bypass
6 authentication procedures” and “failed to employ sufficient measures to detect and prevent
7 unauthorized access to computer networks, such as employing an intrusion detection system and
8 monitoring system logs.”); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006)
9 (“[Defendant] failed to employ sufficient measures to detect unauthorized access.”); *In the*
10 *matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) (“[R]espondent stored . . . personal
11 information obtained to verify checks and process unreceipted returns in clear text on its in-store
12 and corporate networks[,]” “did not require network administrators . . . to use different
13 passwords to access different programs, computers, and networks[,]” and “failed to employ
14 sufficient measures to detect and prevent unauthorized access to computer networks . . .”); *In the*
15 *matter of Dave & Buster’s Inc.*, No. C-4291 (May 20, 2010) (“[Defendant] failed to monitor and
16 filter outbound traffic from its networks to identify and block export of sensitive personal
17 information without authorization” and “failed to use readily available security measures to limit
18 access between instore networks . . .”). These orders, which all preceded the Data Breach, further
19 clarify the measures businesses must take to meet their data security obligations.

20 V. CLASS ACTION ALLEGATIONS

21 5.1 Ms. Waliany sues on behalf of herself and the class (“Class”), defined as follows:

22 All individuals residing in the United States whose personal information was
23 compromised in the Data Breach disclosed by Sea Mar in October 2021.

24 Excluded from the Class are Sea Mar, its agents, affiliates, parents, subsidiaries, any entity in
25 which Sea Mar has a controlling interest, any Sea Mar officer or director, any successor or
26 assign, and any Judge who adjudicates this case, including their staff and immediate family.

1 5.2 Ms. Walianny reserves the right to amend the class definition.

2 5.3 This action satisfies the numerosity, commonality, typicality, and adequacy
3 requirements under CR 23.

4 a. **Numerosity**. Ms. Walianny is a representative of the proposed Class
5 consisting of over 620,000 members—far too many to join in a single action;

6 b. **Ascertainability**. Class members are readily identifiable from information
7 in Sea Mar’s possession, custody, and control;

8 c. **Typicality**. Ms. Walianny’s claims are typical of Class member’s claims as
9 each arises from the same Data Breach, the same alleged negligence and statutory
10 violations by Sea Mar, and the same unreasonable manner of notifying individuals about
11 the Data Breach.

12 d. **Adequacy**. Ms. Walianny will fairly and adequately protect the proposed
13 Class’s interests. Her interests do not conflict with Class members’ interests and she has
14 retained counsel experienced in complex class action litigation and data privacy to
15 prosecute this action on the Class’s behalf, including as lead counsel.

16 e. **Commonality**. Ms. Walianny’s and the Class’s claims raise predominantly
17 common fact and legal questions that a class wide proceeding can answer for all Class
18 members. Indeed, it will be necessary to answer the following questions:

19 i. Whether Sea Mar had a duty to use reasonable care in safeguarding Ms.
20 Walianny and the Class’s PII and PHI;

21 ii. Whether Sea Mar failed to implement and maintain reasonable security
22 procedures and practices appropriate to the nature and scope of the
23 information compromised in the Data Breach;
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

- iii. Whether Sea Mar was negligent in maintaining, protecting, and securing PII and PHI;
- iv. Whether Sea Mar breached contractual promises to safeguard Ms. Waliiany and the Class’s PII and PHI;
- v. Whether Sea Mar took reasonable measures to determine the extent of the Data Breach after discovering it;
- vi. Whether Sea Mar’s Breach Notice was reasonable;
- vii. Whether the Data Breach caused Ms. Waliiany and the Class injuries;
- viii. What is the proper damages measure;
- ix. Whether Sea Mar violated the statutes alleged in this complaint; and
- x. Whether Ms. Waliiany and the Class are entitled to damages, treble damages, or injunctive relief.

5.4 Ms. Waliiany also satisfies the requirements under CR 23(b). Common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

VI. FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Class)

6.1 Plaintiff incorporates all previous paragraphs as if fully set forth below.

6.2 Plaintiff and members of the Class entrusted their PII and PHI to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII and PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data

1 Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at
2 unauthorized access.

3 6.3 Defendant owed a duty of care to Plaintiff and members of the Class because it
4 was foreseeable that Defendant's failure to adequately safeguard their PII and PHI in accordance
5 with state-of-the-art industry standards for data security would result in the compromise of that
6 PII and PHI—just like the Data Breach that ultimately came to pass. Defendant acted with
7 wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of
8 the Class's PII and PHI by disclosing and providing access to this information to third parties and
9 by failing to properly supervise both the way the PII and PHI was stored, used, and exchanged,
10 and those in its employ who made that happen.

11 6.4 Defendant owed to Plaintiff and members of the Class a duty to notify them
12 within a reasonable time frame of any breach to the security of their PII and PHI. Defendant also
13 owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope,
14 nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and
15 members of the Class to take appropriate measures to protect their PII and PHI, to be vigilant in
16 the face of an increased risk of harm, and to take other necessary steps to mitigate the harm
17 caused by the Data Breach.

18 6.5 Defendant owed these duties to Plaintiff and members of the Class because they
19 are members of a well-defined, foreseeable, and probable class of individuals whom Defendant
20 knew or should have known would suffer injury-in-fact from Defendant's inadequate security
21 protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's PII and
22 PHI for medical treatment services. Plaintiff and members of the Class needed to provide their
23 PII and PHI to Defendant to receive medical treatment and services from Defendant, and
24 Defendant retained that information.

25 6.6 The risk that unauthorized persons would try to gain access to the PII and PHI and
26 misuse it was foreseeable. Given that Defendant holds vast amounts of PII and PHI, it was

1 inevitable that unauthorized individuals would try to access Defendant's databases containing the
2 PII and PHI—whether by malware or otherwise.

3 6.7 PII and PHI is highly valuable, and Defendant knew, or should have known, the
4 risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiff and members
5 of the Class's and the importance of exercising reasonable care in handling it.

6 6.8 Defendant breached its duties by failing to exercise reasonable care in supervising
7 its agents, contractors, vendors, and suppliers, and in handling and securing the personal
8 information and PII and PHI of Plaintiff and members of the Class which actually and
9 proximately caused the Data Breach and Plaintiff's and members of the Class's injury. Defendant
10 also breached its duties by failing to provide reasonably timely notice of the Data Breach to
11 Plaintiff and members of the Class, which actually and proximately caused and exacerbated the
12 harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a
13 direct and traceable result of Defendant's negligence or negligent supervision, Plaintiff and
14 members of the Class have suffered or will suffer damages, including monetary damages,
15 increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

16 6.9 Defendant's breach of its common-law duties to exercise reasonable care and its
17 failures and negligence actually and proximately caused Plaintiff's and members of the Class's
18 actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII
19 and PHI by criminals, improper disclosure of their PII and PHI, lost benefit of their bargain, lost
20 value of their PII and PHI, and lost time and money incurred to mitigate and remediate the
21 effects of the Data Breach that resulted from and were caused by Defendant's negligence, which
22 injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

23 **VII. SECOND CLAIM FOR RELIEF**
24 **Breach of Implied Contract**
25 **(On Behalf of Plaintiff and the Class)**

26 7.1. Plaintiff incorporates all previous paragraphs as if fully set forth below.

1 7.2. Defendant offered to provide goods and services to Plaintiff and members of the
2 Class in exchange for payment.

3 7.3. Defendant also required Plaintiff and the members of the Class to provide
4 Defendant with their PII and PHI to receive services.

5 7.4. In turn, and through the Notice of Privacy Practices, Defendant agreed it would
6 not disclose the PHI it collects from patients to unauthorized persons. Defendant also impliedly
7 promised to maintain safeguards to protect its patients' PII and PHI.

8 7.5. Plaintiff and the members of the Class accepted Defendant's offer by providing
9 PII and PHI to Defendant in exchange for receiving Defendant's goods and services and then by
10 paying for and receiving the same.

11 7.6. Implicit in the parties' agreement was that Defendant would provide Plaintiff and
12 members of the Class with prompt and adequate notice of all unauthorized access or theft of their
13 PII and PHI.

14 7.7. Plaintiff and the members of the Class would not have entrusted their PII and PHI
15 to Defendant without such agreement with Defendant.

16 7.8. Defendant materially breached the contract(s) it had entered with Plaintiff and
17 members of the Class by failing to safeguard such information and failing to notify them
18 promptly of the intrusion into its computer systems that compromised such information.
19 Defendant also breached the implied contracts with Plaintiff and members of the Class by:

- 20 a. Failing to properly safeguard and protect Plaintiff's and members of the
21 Class's PII and PHI;
- 22 b. Violating industry standards as well as legal obligations that are
23 necessarily incorporated into the parties' agreement;
- 24 c. Failing to ensure the confidentiality and integrity of electronic PII and PHI
25 that Defendant created, received, maintained, and transmitted in violation
26 of 45 C.F.R. § 164.306(a)(1).

1 7.9 The damages sustained by Plaintiff and members of the Class as described above
2 were the direct and proximate result of Defendant’s material breaches of its agreement(s).

3 7.10 Plaintiff and members of the Class have performed under the relevant agreements,
4 or such performance was waived by the conduct of Defendant.

5 7.11 The covenant of good faith and fair dealing is an element of every contract. All
6 such contracts impose on each party a duty of good faith and fair dealing. The parties must act
7 with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in
8 connection with executing contracts and discharging performance and other duties according to
9 their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently,
10 the parties to a contract are mutually obligated to comply with the substance of their contract
11 along with its form.

12 7.12 Subterfuge and evasion violate the obligation of good faith in performance even
13 when an actor believes their conduct to be justified. Bad faith may be overt or may consist of
14 inaction, and fair dealing may require more than honesty.

15 7.13 Defendant failed to advise Plaintiff and members of the Class of the Data Breach
16 promptly and sufficiently.

17 7.14 In these and other ways, Defendant violated its duty of good faith and fair dealing.

18 7.15 Plaintiff and members of the Class have sustained damages because of
19 Defendant’s breaches of its agreement, including breaches of it through violations of the
20 covenant of good faith and fair dealing.

21 **VIII. THIRD CAUSE OF ACTION**
22 **Violation of the Washington Consumer Protection Act, RCW § 19.86, et seq.**
23 **(On Behalf of the Plaintiff and the Proposed Class)**

24 8.1. Plaintiff incorporates all previous paragraphs as if fully set forth below.

25 8.2. Defendant is a “person” under the Washington Consumer Protection Act, RCW §
26 19.86.101(1), and they conduct “trade” and “commerce” under RCW § 19.86.010(2).

1 8.3. Plaintiff and other members of the proposed Class are “persons” under RCW §
2 19.86.010(1).

3 8.4. Defendant’s failure to safeguard the PII and PHI exposed in the Data Breach
4 constitutes an unfair act that offends public policy.

5 8.5. Defendant’s failure to safeguard the PII and PHI compromised in the Data Breach
6 caused Plaintiff and the proposed Class substantial injury. Defendant’s failure is not outweighed
7 by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable
8 by consumers.

9 8.6. Defendant’s failure to safeguard the PII and PHI disclosed in the Data Breach,
10 and its failure to give time and complete notice of the Data Breach to victims, is unfair because
11 these acts and practices are immoral, unethical, oppressive, and unscrupulous.

12 8.7. Defendant’s unfair acts or practices occurred in its trade or business and have
13 injured and can injure a substantial portion of the public. Defendant’s general conduct as alleged
14 injures the public interest, and the acts Plaintiff complains of are ongoing and have a substantial
15 likelihood of being repeated.

16 8.8. As a direct and proximate result of Defendant’s unfair acts or practices, Plaintiff
17 and the proposed Class suffered an injury in fact.

18 8.9. As a result of Defendant’s conduct, Plaintiff’s and members of the Class’s actual,
19 tangible, injury-in-fact and damages, including, without limitation, the theft of their PHI by
20 criminals, improper disclosure of their PHI, lost benefit of their bargain, lost value of their PHI,
21 and lost time and money incurred to mitigate and remediate the effects of the Data Breach that
22 resulted from and were caused by Defendant’s conduct, which injury-in-fact and damages are
23 ongoing, imminent, immediate, and which they continue to face.

24 8.10. Plaintiff and the proposed Class are entitled to an order enjoining the conduct
25 complained of and ordering Defendant to take remedial measures to prevent similar data
26 breaches; actual damages; treble damages under § 19.86.090; and the costs of bringing this suit,
including reasonable attorney fees.

1 **IX. FOURTH CAUSE OF ACTION**
2 **Violation of the Washington Data Breach Disclosure Law**
3 **(On Behalf of the Plaintiff and the Proposed Class)**

4 9.1. Plaintiff incorporates all previous paragraphs as if fully set forth below.

5 9.2. RCW § 19.255.010(2) provides that “[a]ny person or business that maintains
6 computerized data that includes personal information that the person or business does not own
7 shall notify the owner or licensee of the information of any breach of the security of the data
8 immediately following discovery, if the personal information was, or is reasonably believed to
9 have been, acquired by an unauthorized person.”

10 9.3. The Data Breach led to “unauthorized acquisition of computerized data that
11 compromise[d] the security, confidentiality, [and] integrity of personal information maintained
12 by” Defendant, leading to a “breach of the security of [Defendant’s] systems,” as defined by
13 RCW § 19.255.010.

14 9.4. Defendant failed to disclose that the PII and PHI of hundreds of thousands of
15 patients had been compromised “immediately” upon discovery, and in doing so unreasonably
16 delayed informing Plaintiff and the proposed Class about the Data Breach.

17 **X. FIFTH CAUSE OF ACTION**
18 **Unjust Enrichment**
19 **(On Behalf of the Plaintiff and Proposed Class)**

20 10.1. Plaintiff incorporates all previous paragraphs as if fully set forth below.

21 10.2. This claim is pleaded in the alternative to the breach of implied contractual duty
22 claim.

23 10.3. Plaintiff and members of the Class conferred a monetary benefit upon Defendant
24 in the form of monies paid for treatment services.

25 10.4. Defendant appreciated or knew about the benefits conferred upon itself by
26 Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff’s and
members of the Class’s PHI, as this was used to facilitate payment and treatment services.

10.5. As a result of Defendant’s conduct, Plaintiff, and members of the Class suffered
actual damages in an amount equal to the difference in value between their purchases made with

1 reasonable data privacy and security practices and procedures that Plaintiff and members of the
2 Class paid for, and those purchases without unreasonable data privacy and security practices and
3 procedures that they received.

4 10.6. Under principals of equity and good conscience, Defendant should not be
5 permitted to retain the money belonging to Plaintiff and members of the Class because
6 Defendant failed to implement (or adequately implement) the data privacy and security practices
7 and procedures for itself that Plaintiff and members of the Class paid for and that were otherwise
8 mandated by federal, state, and local laws and industry standards.

9 10.7. Defendant should be compelled to disgorge into a common fund to benefit
10 Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result
11 of the conduct and Data Breach alleged here.

12 **XI. SIXTH CAUSE OF ACTION**
13 **Invasion of Privacy**
14 **(On Behalf of the Plaintiff and Proposed Class)**

15 11.1. Plaintiff incorporates all previous paragraphs as if fully set forth below.

16 11.2. Defendant publicized private details and facts not generally known to the public,
17 not publicly available, and not of legitimate public concern about Plaintiff and Class members by
18 disclosing and exposing Plaintiff's and Class members' private and sensitive PHI and PII to
19 enough people that it is reasonably likely those facts will become known to the public at large,
20 including without limitation on the dark web and elsewhere.

21 11.3. Plaintiff and Class members' PHI and PII, which included patient names,
22 addresses, Social Security numbers, dates of birth, client identification numbers,
23 medical/dental/orthodontic diagnostic and treatment information, medical/vision/dental
24 insurance information, claims information, and/or images associated with dental treatment, was
25 private and intimate.

26 11.4. Defendant's disclosure of the PHI and PII unreasonably, substantially and
seriously interfered with Plaintiff's and Class members' privacy and ordinary sensibilities.
Defendant should appreciate that the cyber-criminals who stole the PHI and PII would further

1 sell and disclose the PII as they are doing and as they did. That the original disclosure is
2 devastating to Plaintiff and Class members even though it may have originally only been made to
3 one person or a limited number of cyber-criminals does not render it any less a disclosure to the
4 public-at-large.

5 11.5. The tort of public disclosure of private facts is recognized in Washington.
6 Plaintiff's and Class members' private and sensitive PHI and PII was publicly disclosed by
7 Defendant in the Data Breach with reckless disregard for the offensiveness of the disclosure.
8 Such disclosure is highly offensive and would be to any person of ordinary sensibilities.
9 Defendant knew and knows that Plaintiff's and Class members' PHI and PII is not a matter of
10 legitimate public concern. As a direct and proximate result of Defendant's conduct, Plaintiff and
11 Class members have been injured and are entitled to damages.

12 XII. PRAYER FOR RELIEF

13 Plaintiff and members of the Class demand a jury trial on all claims so triable and request
14 that the Court enter an order:

- 15 A. Certifying this case as a class action on behalf of Ms. Waliandy and the proposed
16 Class, appointing Ms. Waliandy as class representative, and appointing her counsel
17 to represent the Class;
- 18 B. Awarding declaratory and other equitable relief as is necessary to protect the
19 interests of Ms. Waliandy and the Class;
- 20 C. Awarding injunctive relief as is necessary to protect the interests of Ms. Waliandy
21 and the Class;
- 22 D. Enjoining Sea Mar from further deceptive and unfair practices and making untrue
23 statements about the Data Breach and the stolen PHI;
- 24 E. Awarding Ms. Waliandy and the Class damages that include compensatory,
25 exemplary, punitive damages, and statutory damages, including pre- and post-
26 judgment interest, in an amount to be proven at trial;

- 1 F. Awarding restitution and damages to Plaintiff and the Class in an amount to be
2 determined at trial;
- 3 G. Awarding attorneys' fees and costs, as allowed by law;
- 4 H. Awarding prejudgment and post-judgment interest, as provided by law;
- 5 I. Granting Plaintiff and the Class leave to amend this complaint to conform to the
6 evidence produced at trial; and
- 7 J. Granting such other or further relief as may be appropriate under the
8 circumstances.

9 **JURY DEMAND**

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

11 RESPECTFULLY SUBMITTED AND DATED this 23rd day of December, 2021.

12 **TURKE & STRAUSS LLP**

13 By: /s/ Samuel J. Strauss, WSBA #46971
14 Samuel J. Strauss, WSBA #46971
15 Email: sam@turkestrauss.com
16 936 North 34th Street, Suite 300
17 Seattle, Washington 98103-8869
18 Telephone: (608) 237-1775
19 Facsimile: (608) 509-4423

20 **SMITH & DIETRICH LAW OFFICES PLLC**
21 Walter Smith, WSBA #46695
22 Email: walter@smithdietrich.com
23 3905 Martin Way E., Suite F
24 Olympia, WA 98506
25 Telephone: (360) 915-6952

26 *Attorneys for Plaintiff*

EXHIBIT A

Sea Mar Community Health Centers Notifies Patients of Data Security Incident

SEATTLE, WASHINGTON: October 29, 2021 – Sea Mar Community Health Centers (“Sea Mar”), a non-profit organization that provides healthcare services to underserved communities in the state of Washington, has learned of a data security incident that may have involved personal and protected health information belonging to certain current and former Sea Mar patients. Sea Mar has sent notification of this incident to potentially impacted individuals and has provided resources to assist them.

On June 24, 2021, Sea Mar was informed that certain Sea Mar data had been copied from its digital environment by an unauthorized actor. Upon receipt of this information, Sea Mar immediately took steps to secure its environment and commenced an investigation to determine what happened and to identify the specific information that may have been impacted. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result, Sea Mar learned that additional data may have been removed from its digital environment between December 2020 and March 2021. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals, which was completed on August 30, 2021.

Sea Mar is not aware of any evidence of the misuse of any information potentially involved in this incident. However, beginning on October 29, 2021, Sea Mar provided of this incident to the potentially impacted individuals. In so doing, Sea Mar provided information about the incident and about steps that potentially impacted individuals can take to protect their information. Sea Mar takes the security and privacy of patient information very seriously and is taking steps to prevent a similar event from occurring in the future.

The following personal and protected health information may have been involved in the incident: Name, 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.

Sea Mar has established a toll-free call center to answer questions about the incident and to address related concerns. Call center representatives are available Monday through Friday between 6:00 am – 3:30 pm Pacific Time and can be reached at 1-855-651-2684.

The privacy and protection of personal and protected health information is a top priority for Sea Mar, which deeply regrets any inconvenience or concern this incident may cause.

While we are not aware of the misuse of any potentially affected individual’s information, we are providing the following information to help those wanting to know more about steps they can take to protect themselves and their personal information:

What steps can I take to protect my personal information?

- Please notify your financial institution immediately if you detect any suspicious activity on any of your accounts, including unauthorized transactions or new accounts opened in our name that you do not recognize. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities.
- You can request a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To do so, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is listed at the bottom of this page.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC’s website offers helpful information at www.ftc.gov/idtheft.
- Additional information on what you can do to better protect yourself is included in your notification letter.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Use the following contact information for the three nationwide credit reporting agencies:

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

How do I put a fraud alert on my account?

You may consider placing a fraud alert on your credit report. This fraud alert statement informs creditors to possible fraudulent activity within your report and requests that your creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is included in the letter and is also listed at the bottom of this page.

How do I put a security freeze on my credit reports?

You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or online by following the instructions found at the websites listed below. You will need to provide the following information when requesting a security freeze (note that if you are making a request for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) address. You may also be asked to provide other personal information such as your email address, a copy of a government-issued identification card, and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. There is no charge to place, lift, or remove a freeze. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

Experian Security Freeze
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion (FVAD)
PO Box 2000
Chester, PA 19022
1-800-909-8872
www.transunion.com

What should I do if my family member was involved in the incident and is deceased?

You may choose to notify the three major credit bureaus, Equifax, Experian and Trans Union, and request they flag the deceased credit file. This will prevent the credit file information from being used to open credit. To make this request, mail a copy of your family member's death certificate to each company at the addresses below.

Equifax
Equifax Information Services
P.O. Box 105169,
Atlanta, GA 30348

Experian
Experian Information Services
P.O. Box 9701
Allen, TX 75013

TransUnion
Trans Union Information
Services
P.O. Box 2000
Chester, PA 19022