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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

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

1.6 On August 31, 2021, Sea Mar concluded its internal investigation, but it still did 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").

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

II. PARTIES

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

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

III. JURISDICTION AND VENUE

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

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

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

//

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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).

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

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

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

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

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

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

[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).

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

4.14 Marketo included a "Bids counter" which purportedly tracked how many bids the patients' PII and PHI had received.

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

[4] *Id.*

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

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

4.20 According to Sea Mar, its internal investigation revealed that it lost control over patients' PII and PHI, including photos from patient procedures: "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."

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

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

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

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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

4.26 Instead, Sea Mar's Breach Notice hid the disturbing nature of the Data Breach, misrepresenting that Sea Mar "ha[d] no evidence that any potentially affected information has been misused."

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

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

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

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

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

D. Plaintiff's Experience

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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

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

E. Ms. Waliany and the Proposed Class Face Significant Risk of Identity Theft

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

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

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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

a. The loss of the opportunity to control how their PII and PHI are used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII and PHI; and

h. The continued risk to their PII and PHI, which remains in the possession of Sea Mar and is subject to further breaches so long as Sea Mar fails to undertake the appropriate measures to protect the PII and PHI in their possession.

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

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

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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

4.45 One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.

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

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

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

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

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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

4.55 According to the FTC, unauthorized PHI disclosures are extremely damaging to 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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

V. CLASS ACTION ALLEGATIONS

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

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

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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

5.2 Ms. Waliany reserves the right to amend the class definition.

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

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

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

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

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

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

i. Whether Sea Mar had a duty to use reasonable care in safeguarding Ms. Waliany and the Class's PII and PHI;

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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

iii. Whether Sea Mar was negligent in maintaining, protecting, and securing PII and PHI;

iv. Whether Sea Mar breached contractual promises to safeguard Ms. Waliany 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. Waliany 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. Waliany and the Class are entitled to damages, treble damages, or injunctive relief.

5.4 Ms. Waliany 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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

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

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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

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

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

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

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PII and PHI;

b. Violating industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic PII and PHI that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

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

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

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

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

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

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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

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

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

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

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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

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

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

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

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

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

10.4. Defendant appreciated or knew about the benefits conferred upon itself by 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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

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

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

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

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

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

XII. PRAYER FOR RELIEF

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

A. Certifying this case as a class action on behalf of Ms. Waliany and the proposed Class, appointing Ms. Waliany as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Ms. Waliany and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Ms. Waliany and the Class;

D. Enjoining Sea Mar from further deceptive and unfair practices and making untrue statements about the Data Breach and the stolen PHI;

E. Awarding Ms. Waliany and the Class damages that include compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest, in an amount to be proven at trial;

TURKE & STRAUSS LLP
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

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

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

TURKE & STRAUSS LLP

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

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

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	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-800-685-1111
www.transunion.com	www.experian.com	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	Experian Security Freeze	TransUnion (FVAD)
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-909-8872
www.equifax.com	www.experian.com	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	**Experian**	**TransUnion**
Equifax Information Services	Experian Information Services	Trans Union Information
P.O. Box 105169,	P.O. Box 9701	Services
Atlanta, GA 30348	Allen, TX 75013	P.O. Box 2000
		Chester, PA 19022