IN THE UNITED STATE DISTRICT COURT

FOR THE WESTERN DISTRICT OF WASHINGTON

SEATTLE DIVISION

MARIA BARNES and DEREK GANNON, individually and on behalf of all others similarly situated, Plaintiffs 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. 21-2-15063-9 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. 21-2-15063-9 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, *Maria Barnes and Derek Gannon, individually*

LEWIS BRISBOIS BISGAARD & SMITH LLP
1111 Third Avenue, Suite 2700
Seattle, Washington 98101
206.436.2020

and on behalf of all others similarly situated v. Sea Mar Community Health Centers, was filed in King County Superior Court, State of Washington, on November 12, 2021. A true and correct copy of the Class Action Complaint filed in King County Superior Court Case No: 21-2-15-130-9 SEA is attached as **Exhibit A**. This is a civil action arising out of allegations of negligence per se violations of (1) HIPAA 45 C.F.R. § 160 and § 164, (2) unfair trade practices pursuant to FTC Act 15 U.S.C. § 45(a)(1), (3) RCW 19.86.101 Washington Consumer Protection Act; as well as allegations of (4) negligence, (5) breach of fiduciary duty, (6) breach of express contract, (7) breach of implied contract, (8) unjust enrichment, and (9) breach of implied covenant of good faith and fair dealing, with claims made by Plaintiffs for actual damages, punitive damages, restitution, disgorgement, credit monitoring, attorney fees and costs, equitable, declaratory and injunctive relief.

II. GROUNDS FOR REMOVAL

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

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

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

B. The Federal Tort Claims Act, 28 U.S.C. 1346(b) Applies to Plaintiffs' Claims.

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

LEWIS BRISBOIS BISGAARD & SMITH LLP
1111 Third Avenue, Suite 2700
Seattle, Washington 98101
206.436.2020

> Subject to the provisions of chapter 171 of this title, the district courts . . . shall have exclusive jurisdiction of civil actions against the United States . . . for injury or loss of property, or personal injury or death caused by the negligent or wrongful act or omission of any employee of the Government while acting within the scope of his office or employment, under circumstances where the United States, if a private person, would be liable to the claimant in accordance with the law of the place where the act or omission occurred.

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

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

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

D. Sea Mar's Conduct Was Function Required and Related to the Provision of Medical Care.

To facilitate medical care, Sea Mar—like any doctor's office—creates medical records, and collects and maintains personal information from its patients. The maintenance, retention, 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

LEWIS BRISBOIS BISGAARD & SMITH LLP
1111 Third Avenue, Suite 2700
Seattle, Washington 98101
206.436.2020

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

III. TIME FOR REMOVAL

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

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

IV. REQUIRED DOCUMENTS

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

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

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

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

/ / /

/ / /

LEWIS BRISBOIS BISGAARD & SMITH LLP
1111 Third Avenue, Suite 2700
Seattle, Washington 98101
206.436.2020

DATED: February 16, 2022

LEWIS BRISBOIS BISGAARD & SMITH LLP

s/Kathleen A. Nelson
Kathleen A. Nelson, WSBA #22826

s/Randy J. Aliment
Randy J. Aliment, WSBA #11440

s/Aryn M. Seiler
Aryn M. Seiler, WSBA #57270

1111 Third Avenue, Suite 2700
Seattle, Washington 98101
(206) 436-2020 / (206)436-2030 Fax
Kathleen.Nelson@lewisbrisbois.com
Randy.Aliment@lewisbrisbois.com
Aryn.Seiler@lewisbrisbois.com
Attorneys for Defendant

DECLARATION OF SERVICE

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

Alexander F. Strong, WSBA #49839 Bendich Stobaugh & Strong, PC 126 NW Canal Street, Suite 100 Seattle, WA 98107 (206) 622-3536 ***Attorney for Plaintiff***	☐ via U.S. Mail, first class, postage prepaid ☐ via Legal Messenger Hand Delivery ☐ via Facsimile ☒ via CM/ECF ☒ via E-mail: astrong@bs-s.com aforsgaard@bs-s.com cfaltesek@bs-s.com
Ben Barnow Anthony L. Parkhill Barnow & Associates, PC 205 West Randolph Street, Ste. 1630 Chicago, IL 60606 (312) 621-2000 ***Attorney for Plaintiff***	☐ via U.S. Mail, first class, postage prepaid ☐ via Legal Messenger Hand Delivery ☐ via Facsimile ☒ via CM/ECF ☒ via E-mail: b.barnow@barnowlaw.com aparkhill@barnowlaw.com rprince@barnowlaw.com
Tina Wolfson Robert Ahdoot Ahdoot & Wolfson, PC 2600 W. Olive Avenue, Suite 500 Burbank, CA 91505-4521 (310) 474-8585 ***Attorney for Plaintiff***	☐ via U.S. Mail, first class, postage prepaid ☐ via Legal Messenger Hand Delivery ☐ via Facsimile ☒ via CM/ECF ☒ via E-mail: twolfson@ahdootwolfson.com rahdoot@ahdootwolfson.com
Andrew W. Ferich Ahdoot & Wolfson, PC 201 King of Prussia Road, Suite 650 Radnor, PA 19087 (310) 474-9111 ***Attorney for Plaintiff***	☐ via U.S. Mail, first class, postage prepaid ☐ via Legal Messenger Hand Delivery ☐ via Facsimile ☒ via CM/ECF ☒ via E-mail: aferich@ahdootwolfson.com hlivamagi@ahdootwolfson.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 ***United States Attorneys***	☐ via U.S. Mail, first class, postage prepaid ☐ via Legal Messenger Hand Delivery ☐ via Facsimile ☒ via CM/ECF ☒ via E-mail: kristen.vogel@usdoj.gov

Dated February 16, 2022 at Seattle, Washington.

s/ Annie Kliemann

Annie Kliemann
Annie.Kliemann@lewisbrisbois.com

EXHIBIT A

FILED
2021 NOV 12 09:00 AM
KING COUNTY
SUPERIOR COURT CLERK
E-FILED
CASE #: 21-2-15063-9 SEA

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

MARIA BARNES and DEREK GANNON, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

SEA MAR COMMUNITY HEALTH CENTERS,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Maria Barnes and Derek Gannon ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through their attorneys, bring this Class Action Complaint against Defendant Sea Mar Community Health Centers ("Sea Mar") and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Sea Mar for its failure to secure and safeguard their and approximately 651,500 other individuals' private and confidential medical information, including: names; addresses; Social Security numbers; dates of birth; client

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

identification numbers; medical, vision, dental, and/or orthodontic diagnostic and treatment information; medical, vision, and/or dental insurance information; claims information; and/or images associated with dental treatment ("PII/PHI").

2. Defendant is an organization consisting of health centers around Washington state. The organization has health centers in twelve different counties in Washington.

3. Between December 2020 and March 2021, unauthorized individuals gained access to Sea Mar's computer network and accessed and copied the PII/PHI of Plaintiffs and Class members (the "Data Breach").

4. Sea Mar owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Sea Mar breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' PII/PHI from unauthorized access and disclosure.

5. As a result of Sea Mar's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all Washington residents whose PII/PHI was exposed as a result of the Data Breach, which Sea Mar learned of on June 24, 2021 and first publicly acknowledged on October 29, 2021, over four months after the breach was discovered.

6. Plaintiffs, on behalf of themselves and all other Class members, assert claims for negligence, negligence per se, breach of fiduciary duty, breach of express contract, breach of implied contract, unjust enrichment, breach of implied covenant of good faith and fair dealing, and

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

violation of the Washington Consumer Protection Act and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

7. Plaintiff Maria Barnes is a Washington resident who received health services at a Sea Mar Community Health Centers facility. Believing Sea Mar would implement and maintain reasonable security and practices to protect her PII/PHI, Plaintiff Barnes routinely provided her PII/PHI to Sea Mar in connection with receiving health services. Plaintiff Barnes received a letter from Sea Mar notifying her that her PII/PHI may have been exposed in the Data Breach. Had Plaintiff Barnes known that Sea Mar does not adequately protect PII/PHI, she would not have used Sea Mar's services and agreed to provide Sea Mar with her PII/PHI.

8. Plaintiff Derek Gannon is a Washington resident who received health services at a Sea Mar Community Health Centers facility. Believing Sea Mar would implement and maintain reasonable security and practices to protect his PII/PHI, Plaintiff Gannon routinely provided his PII/PHI to Sea Mar in connection with receiving health services. Plaintiff Gannon received a letter from Sea Mar notifying him that his PII/PHI may have been exposed in the Data Breach. Following receipt of the notification letter, Plaintiff Gannon has spent approximately a half hour checking his credit in order to determine if he has been the victim of fraud. Had Plaintiff Gannon known that Sea Mar does not adequately protect PII/PHI, he would not have used Sea Mar's services and agreed to provide Sea Mar with his PII/PHI.

9. Defendant Sea Mar Community Health Centers is a non-profit corporation incorporated in Washington and has locations throughout Washington. Sea Mar's corporate

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

headquarters are located at 1040 S. Henderson Street, Seattle, WA 98108.

JURISDICTION AND VENUE

10. This Court has jurisdiction over this matter pursuant to RCW 2.08.010.

11. This Court has personal jurisdiction over Sea Mar because Sea Mar is a corporation organized under the laws of Washington and has its principal place of business in Washington.

12. Venue is proper in King County pursuant to RCW 4.12.020 and RCW 4.12.025 because Sea Mar's principal place of business is located in King County.

FACTUAL ALLEGATIONS

Overview of Sea Mar

13. Sea Mar is an organization that has over 90 health clinics in Washington, providing medical, dental, and behavioral health services. In its annual report from 2020, the company stated that it served over 300,000 patients between April 1, 2019 and March 31, 2020.[1]

14. In the regular course of its business, Sea Mar collects and maintains the PII/PHI of patients, former patients, and other persons to whom it is currently providing or previously provided health-related services.

15. Sea Mar requires patients to provide personal information before it provides treatment at its facilities and requires employees to provide information before being hired and participating in its health plan. That information includes, *inter alia*, names, addresses, dates of birth, health insurance information, and Social Security numbers. Sea Mar also creates, collects, and stores other PII/PHI of its patients and former patients, including client identification numbers

[1] Sea Mar Community Health Centers, *Report to the Community 2020*, SEAMAR.ORG, https://www.seamar.org/seamar-downloads/Annual-Report2020.pdf (last accessed Nov. 9, 2021).

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

and medical information. Sea Mar stores this information digitally.

16. Sea Mar's website contains a page entitled, "Notice of Privacy Practices," which states, "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."[2]

17. Plaintiffs and Class members are, or were, patients of Sea Mar or received health-related services from Sea Mar, and entrusted Sea Mar with their PII/PHI.

The Data Breach

18. In or about December of 2020, an unauthorized individual, or unauthorized individuals, gained access to Sea Mar's network system. Sea Mar states in its notice that on June 24, 2021, the company was "informed that certain Sea Mar data had been copied from its digital environment by an unauthorized actor."[3] One website, DataBreaches.net, claims to have sent inquiries to Sea Mar on June 24, 2021, warning the company that three terabytes of its data was for sale on the dark web.[4]

19. Plaintiffs and the Class members' information is now available to cybercriminals on the dark web and there were already over 200 bids to purchase their information in July.[5]

20. Sea Mar did not begin to notify government agencies or the public about the data

---

[2] *See* Sea Mar Community Health Centers, *Notice Privacy Practices*, SEAMAR.ORG, https://www.seamar.org/notice.html (last accessed Nov. 9, 2021).

[3] Sea Mar Community Health Centers, *Sea Mar Community Health Centers Notifies Patients of Data Security Incident* ("Notice"), SEAMAR.ORG, https://www.seamar.org/seamar-downloads/2021-10-28-Breach_Notice.pdf (last accessed Nov. 9, 2021).

[4] DataBreaches.net, *WA: Sea Mar Community Health Centers Discloses Breach That Began Last Year* (October 30, 2021), https://www.databreaches.net/wa-sea-mar-community-health-centers-discloses-breach-that-began-last-year/ (last accessed Nov. 9, 2021).

[5] *Id*.

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

breach until over four months after it was warned of the data breach, on or about October 29, 2021. The notice that Sea Mar posted on its website states the information that was accessed included:

> 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.[6]

Sea Mar Knew that Criminals Target PII/PHI

21. At all relevant times, Sea Mar knew, or should have known, its patients', Plaintiffs', and all other Class members' PII/PHI was a target for malicious actors. Despite such knowledge, Sea Mar failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII/PHI from cyber-attacks that Sea Mar should have anticipated and guarded against.

22. It is well known amongst companies that store sensitive personally identifying information that sensitive information—like the Social Security numbers ("SSNs") and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[7]

23. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were

---

[6] *See* Notice, supra at n.3

[7] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

758 medical data breaches in 2020 with over 40 million patient records exposed.[8] This is an increase from the 572 medical data breaches that Protenus compiled in 2019.[9]

24. PII/PHI is a valuable property right.[10] The value of PII/PHI as a commodity is measurable.[11] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[12] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[13] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

25. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This

---

[8] Protenus, *2021 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2021-breach-barometer (last accessed Nov. 10, 2021).

[9] Protenus, *2020 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/resources/2020-breach-barometer (last accessed Nov. 10, 2021).

[10] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data (last accessed Nov. 10, 2021)

[11] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

[12] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[13] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

26. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[14] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[15] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[16]

27. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[17] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[18]

---

[14] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[15] *Id.*

[16] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

[17] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[18] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last accessed Nov. 2, 2021).

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

28. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[19] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[20]

29. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[21]

30. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

31. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[22]

---

[19] *What Happens to Stolen Healthcare Data*, *supra* at n.14.
[20] *Id.*
[21] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.
[22] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 10, 2021).

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

32. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[23] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[24]

33. With access to an individual's PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's

[23] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[24] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Nov. 10, 2021).

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

name.[25]

34. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[26]

35. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

36. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[27]

37. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[28] It "is also more difficult to detect,

---

[25] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 10, 2021).
[26] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Nov. 10, 2021).
[27] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[28] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

taking almost twice as long as normal identity theft."[29] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [30] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[31]

38. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.

---

[29] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.18.
[30] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Nov. 10, 2021).
[31] *Id.*

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[32]

39. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[33]

40. It is within this context that Plaintiffs and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiffs and the Other Class Members

41. Plaintiffs and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

---

[32] *See* Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at 28.
[33] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

CLASS ALLEGATIONS

42. This action is brought and may be properly maintained as a class action pursuant to Washington Superior Court Civil Rule 23.

43. Plaintiffs bring this action on behalf of themselves and all members of the following Class of similarly situated persons:

> All Washington residents whose PHI/PII was accessed by and disclosed to unauthorized persons in the Data Breach, including all Washington residents who were sent a notice of the Data Breach.

44. Excluded from the Class is Sea Mar Health Centers and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

45. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

46. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Sea Mar reported to the Maine Attorney General that approximately 651,500 individuals' information was exposed in the Data Breach.

47. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Sea Mar had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PII/PHI from unauthorized access and disclosure;

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

b. Whether Sea Mar failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII/PHI;

c. Whether an implied contract existed between Class members and Sea Mar providing that Sea Mar would implement and maintain reasonable security measures to protect and secure Class Members' PII/PHI from unauthorized access and disclosure;

d. Whether Sea Mar breached its duties to protect Plaintiffs' and Class member's PII/PHI; and

e. Whether Plaintiffs and all other members of the Class are entitled to damages and the measure of such damages and relief.

48. Sea Mar engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

49. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Sea Mar, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

50. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiffs have retained counsel with

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

51. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Sea Mar, so it would be impracticable for Class members to individually seek redress from Sea Mar's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

52. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

53. Sea Mar owed a duty to Plaintiffs and all other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

54. Sea Mar knew the risks of collecting and storing Plaintiffs' and all other Class members' PII/PHI and the importance of maintaining secure systems. Sea Mar knew of the

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

many data breaches that targeted healthcare providers in recent years, including breaches of Sea Mar data.

55. Given the nature of Sea Mar's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Sea Mar should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

56. Sea Mar breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiffs' and Class members' PII/PHI.

57. It was reasonably foreseeable to Sea Mar that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

58. But for Sea Mar's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their PII/PHI would not have been compromised.

59. As a result of Sea Mar's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT II

NEGLIGENCE PER SE

60. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

61. Sea Mar's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

62. Sea Mar's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Sea Mar, of failing to employ reasonable measures to protect and secure PII/PHI.

63. Sea Mar violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other Class members' PII/PHI and not complying with applicable industry standards. Sea Mar's conduct was

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class members.

64. Sea Mar's violation of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

65. Plaintiffs and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

66. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and all other Class members as a result of the Data Brach.

67. It was reasonably foreseeable to Sea Mar that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

68. The injury and harm that Plaintiffs and Class members suffered was the direct and proximate result of Sea Mar's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT III

BREACH OF FIDUCIARY DUTY

69. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

70. Plaintiffs and Class members gave Sea Mar their PII/PHI in confidence, believing that Sea Mar would protect that information. Plaintiffs and Class members would not have provided Sea Mar with this information had they known it would not be adequately protected. Sea Mar's acceptance and storage of Plaintiffs' and Class members' PII/PHI created a fiduciary relationship between Sea Mar and Plaintiffs and Class members. In light of this relationship, Sea Mar must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiffs' and Class members' PII/PHI.

71. Sea Mar has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

failing to safeguard Plaintiffs' and Class members' PII/PHI that it collected.

72. As a direct and proximate result of Sea Mar's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Sea Mar's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach.

COUNT IV

BREACH OF EXPRESS CONTRACT

73. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

74. Plaintiffs and Class members and Sea Mar entered into written agreements together regarding the medical care or other services that Sea Mar was to provide to Plaintiffs and Class members upon Plaintiff and Class members receiving medical services at Sea Mar facilities. One such agreement is the Notice of Privacy Practices, which states that Defendant "will not disclose [patients'] information to others unless [the patients] tell us to do so, or unless the law authorizes or requires us to do so." Plaintiffs and Class members paid Sea Mar monies and provided Sea Mar with their PII/PHI as consideration for these agreements, directly or through an insurance carrier.

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

75. Plaintiffs and Class members complied with the express contract when they paid Sea Mar, directly or through an insurance carrier.

76. Sea Mar breached its obligations under the contract between itself and Plaintiffs and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI.

77. Sea Mar's breach of the express contract between itself, on the one hand, and Plaintiffs and Class members, on the other hand directly caused the Data Breach.

78. Plaintiffs and all other Class members were damaged by Sea Mar's breach of express contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT V

BREACH OF IMPLIED CONTRACT

79. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

80. In connection with receiving medical treatment or services, Plaintiffs and all other Class members entered into implied contracts with Sea Mar.

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

81. Pursuant to these implied contracts, Plaintiffs and Class members paid money to Sea Mar, whether directly or through their insurers, and provided Sea Mar with their PII/PHI. In exchange, Sea Mar agreed to, among other things, and Plaintiffs understood that Sea Mar would: (1) provide medical treatment pr services to Plaintiffs and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII/PHI; and (3) protect Plaintiffs' and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

82. The protection of PII/PHI was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Sea Mar, on the other hand. Indeed, as set forth *supra*, Sea Mar recognized the importance of data security and the privacy of its patients' PII/PHI in its Notice of Privacy Practices. Had Plaintiffs and Class members known that Sea Mar would not adequately protect its patients' PII/PHI, they would not have received medical treatment or services from Sea Mar.

83. Plaintiffs and Class members performed their obligations under the implied contract when they provided Sea Mar with their PII/PHI and paid—directly or through their insurers—for health care treatment or services from Sea Mar.

84. Sea Mar breached its obligations under its implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

85. Sea Mar's breach of its obligations of its implied contracts with Plaintiffs and

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

86. Plaintiffs and all other Class members were damaged by Sea Mar's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT VI

UNJUST ENRICHMENT

87. Plaintiffs reallege and incorporate by reference paragraphs 1–51 as if fully set forth herein.

88. This claim is pleaded in the alternative to the breach of express and implied contract claims.

89. Plaintiffs and Class members conferred a monetary benefit upon Sea Mar in the form of monies paid for health care services.

90. Sea Mar accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Sea Mar also benefitted from the receipt of Plaintiffs' and Class members' PHI, as this was used to facilitate payment.

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

91. As a result of Sea Mar's conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

92. Sea Mar should not be permitted to retain the money belonging to Plaintiffs and Class members because Sea Mar failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

93. Sea Mar should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VII

BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

94. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

95. All contracts contain an implied covenant of good faith and fair dealing.

96. As alleged above, Plaintiffs and Class members entered into express and implied contracts with Sea Mar for medical or other related services and in exchange provided Sea Mar with their PII/PHI and monies, paid directly or through and insurer.

97. As a part of those contracts, Sea Mar promised to safeguard the PII/PHI of Plaintiffs and Class members and Plaintiffs and Class members expected Sea Mar to safeguard

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

that information.

98. Sea Mar breached the implied covenant of good faith and fair dealing by not adequately safeguarding Plaintiffs' and Class members' PII/PHI.

99. Plaintiffs and all other Class members were damaged by Sea Mar's breach of the implied covenant of good faith and fair dealing because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT VIII

VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT RCW §§ 19.86.010 et seq. ("WCPA")

100. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

101. Plaintiffs and Sea Mar are "persons" under the WCPA. RCW § 19.86.010(1).

102. Sea Mar's sale of medical and other health care services to Plaintiffs and all other Class members constitutes as "trade" and "commerce" under the WCPA. RCW § 19.86.010(2).

103. The WCPA states, "Unfair methods of competition and unfair or deceptive

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

practices in the conduct of any trade or commerce are hereby declared unlawful." RCW § 19.86.020. Sea Mar's failure to adequately safeguard Plaintiffs and Class members PII/PHI while representing that their PII/PHI would be protected is an "unfair or deceptive practice" under the WCPA.

104. Had Plaintiffs and the other Class members been aware of the omitted and misrepresented facts, i.e., that Sea Mar would not adequately protect their PII/PHI, Plaintiffs and the other Class members would not have sought medical or other health care services from Sea Mar.

105. Pursuant to RCW § 19.86.090, Plaintiffs seeks actual and treble damages on behalf of themselves and all other Class members.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in their favor and against Sea Mar as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent Sea Mar from experiencing another data breach by adopting and implementing best data security practices to

BENDICH, STOBAUGH & STRONG, P.C.
126 NW CANAL STREET, SUITE 100
SEATTLE, WASHINGTON 98107
(206) 622-3536

safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: November 11, 2021

Respectfully submitted,

/s/ Alexander F. Strong
ALEXANDER F. STRONG, WSBA #49839
astrong@bs-s.com
BENDICH STOBAUGH & STRONG, PC
126 NW Canal Street, Suite 100
Seattle, WA 98107
Telephone: (206) 622-3536
Facsimile: (206) 622-5759

BEN BARNOW*
b.barnow@barnowlaw.com
ANTHONY L. PARKHILL*
aparkhill@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504

TINA WOLFSON*
twolfson@ahdootwolfson.com
ROBERT AHDOOT*
rahdoot@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

ANDREW W. FERICH*
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

**pro hac vice* to be submitted