LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

November 5, 2021

VIA ONLINE SUBMISSION
Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

We represent Sea Mar Community Health Centers ("Sea Mar"), a healthcare provider located in the state of Washington, in connection with a data security incident described in greater detail below. This letter is being sent because the personal information of certain Maine residents may have been affected by a recent data security incident experienced by Sea Mar. The incident may have involved unauthorized access to the Maine residents' names and Social Security numbers.

On June 24, 2021, Sea Mar was informed that certain Sea Mar data had been removed from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately took steps to secure its environment and commenced an investigation to determine what happened. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of this independent investigation, Sea Mar learned on August 12, 2021 that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

On October 22, 2021, Sea Mar learned of six (6) Maine residents within the potentially affected population whose personal information may have been affected as a result of the incident. An additional fifty-two (52) residents were notified pursuant to the Health Insurance Portability and Accountability Act of 1996.

Sea Mar notified the potentially affected Maine residents of this incident via the attached sample letter(s) beginning on October 29, 2021. In so doing, Sea Mar offered notified individuals whose Social Security numbers may have been involved complimentary identity protection services through

Kroll, a global leader in risk mitigation and response. Sea Mar has also reported this incident to the Federal Bureau of Investigation.

Please contact me should you have any questions.

Very truly yours,

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Consumer Notification Letter

Sea Mar
Community Health Centers
Clínica de la Comunidad
Exceptional service. Every person. Every time.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Data <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers ("Sea Mar") that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident, steps that you can take to help protect your information, and resources that Sea Mar is making available to assist you.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your 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 may have been impacted in connection with this incident.

What We Are Doing. As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

To help relieve concerns and to help safeguard your identity following this incident, Sea Mar has secured the services of Kroll to provide identity monitoring services at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services include Credit Monitoring, Web Watcher, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until **January 27, 2022** to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

Additional information describing your services is included with this letter.

What You Can Do. Sea Mar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

Sea Mar also encourages you to take full advantage of the services offered to you through Kroll. Kroll representatives are available to answer questions or address concerns you may have. Kroll call center representatives are available Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holiday; and can be reached by calling 1-855-651-2684.

For More Information. If you have questions or need assistance, please call 1-855-651-2684, Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays. Please accept our sincere apologies and know that Sea Mar deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Rogelio Riojas, Executive Director

Sea Mar Community Health Centers
1040 S. Henderson Street
Seattle, Washington 98108

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

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

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

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Sea Mar
Community Health Centers
Clínica de la Comunidad
Exceptional service. Every person. Every time.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Data <<b2b_text_1(Header)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a data security incident recently discovered by Sea Mar Community Health Centers ("Sea Mar") that may have impacted your personal / protected health information. Sea Mar takes the privacy and security of all patient information very seriously. This letter contains information about the recent incident and steps that you can take to help protect your information.

What Happened? On June 24, 2021, Sea Mar was informed that certain data belonging thereto had been copied from the Sea Mar digital environment. Upon receipt of this information, Sea Mar immediately undertook efforts to secure its environment and commenced an internal investigation to determine what happened and to identify the specific information that may have been involved. In so doing, Sea Mar engaged leading, independent cybersecurity experts for assistance. As a result of its investigation, Sea Mar learned on August 12, 2021, that additional data may have been copied from the Sea Mar digital environment between December 2020 and March 2021, and that such data may have contained personal / protected health information belonging to Sea Mar patients. Sea Mar thereafter began collecting contact information needed to provide notice to potentially affected individuals. This process was completed on August 30, 2021.

Sea Mar has no evidence that any potentially affected information has been misused. Nonetheless, Sea Mar is sending this letter to notify you about the incident and to provide information about steps that you can take to help protect your personal / protected health information.

What Information Was Involved? Sea Mar determined that your name, address, 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 may have been impacted in connection with this incident.

What We Are Doing. As soon as Sea Mar discovered this incident, Sea Mar took the steps described above. Sea Mar also began working with cybersecurity experts to identify areas in which it can further improve the security of its network to reduce the likelihood of a similar event occurring in the future. Additionally, Sea Mar reported this incident to the Federal Bureau of Investigation and will provide any cooperation necessary to hold the perpetrators of this incident accountable.

What You Can Do. Sea Mar encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits forms, and to monitor your free credit reports for suspicious activity and to detect errors. You can also follow the recommendations included with this letter to help protect your information.

For More Information. Further information about how to help protect your personal information is included with this letter. If you have questions or need assistance, please contact 1-855-651-2684, Monday through Friday, 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays. Our representatives are fully versed on this incident and can answer any questions you may have.

Please accept our sincere apologies and know that Sea Mar deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Rogelio Riojas, Executive Director

Sea Mar Community Health Centers
1040 S. Henderson Street
Seattle, Washington 98108

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

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

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

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.