RECEIVED
APR 01 2024
CONSUMER PROTECTION

LEWIS BRISBOIS
LEWIS BRISBOIS BISGAARD & SMITH LLP

March 26, 2024

Via electronic-mail: *DOJ-CPB@doj.nh.gov*; *AttorneyGeneral@doj.nh.gov*

Attorney General John Formella
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Our Client : Saco River Medical Group
Matter : Data Security Incident on March 7, 2024

Dear Attorney General Formella:

We represent Saco River Medical Group ("SRMG") with a principal place of business in Conway, New Hampshire with respect to a potential data security incident described in more detail below. SRMG takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of New Hampshire residents that were potentially affected, what information has been compromised, and the steps that SRMG is taking in response to this incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On or about March 7, 2024, SRMG learned that fraudulent tax returns were filed for several of its employees. Upon learning of the incident, SRMG immediately confirmed that its network was secure, and launched an internal investigation.

The investigation remains ongoing. However, out of an abundance of caution, SRMG is notifying current and former employees about the incident. Because fraudulent tax returns were filed, it is possible that an unauthorized third party may have accessed individuals' personal information, including

2. New Hampshire Residents Notified

A total of and forty-three (43) residents of New Hampshire were potentially affected by this security incident. A notification letter to these individuals will be mailed on March 26, 2024, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

The security and privacy of personal data remains one of SRMG's highest priorities. SRMG is taking steps to prevent a similar event from occurring in the future by implementing additional safeguards and enhanced security measures to better protect the privacy and security of information in its systems. SRMG has also reviewed and taken steps to enhance its policies and procedures relating to the security of its systems, as well as its information life cycle management.

SRMG has also extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through Cyberscout. This service will include of credit monitoring, along with a fully managed identity theft recovery service, should the need arise. The notification letter and offer of free credit monitoring will be mailed on March 26, 2024.

4. Contact Information

SRMG remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at

Very truly yours,

Lewis Brisbois Bisgaard & Smith, LLC

Tawana Johnson, Esq.

cc: Robert Walker, Esq.
(Lewis Brisbois LLC)

Enclosures: *Sample notification letter*

Saco River Medical Group
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08666

SACO RIVER MEDICAL GROUP

[redacted]

March 26, 2024

Via First-Class Mail

Notice of Data Security Incident

Dear [redacted],

Saco River Medical Group ("SRMG") is a primary care and non-emergent walk-in clinic located in Conway, New Hampshire. You are receiving this letter because you are a current or former employee of SRMG. We are writing to inform you of an incident that may have exposed your personal information. We take the privacy of your personal information seriously and want to provide you with information and resources you can use to protect your personal information.

What Happened and What Information was Involved:

On or about March 7, 2024, SRMG learned that fraudulent tax returns were filed for several of its employees. Upon learning of the incident, SRMG immediately confirmed that its network was secure, and launched an internal investigation.

The investigation remains ongoing. However, out of an abundance of caution, SRMG is notifying current and former employees about the incident. Because fraudulent tax returns were filed, it is possible that an unauthorized third party may have accessed your personal information, including your

What We Are Doing:

The security and privacy of personal data remains one of SRMG's highest priorities. SRMG is taking steps to prevent a similar event from occurring in the future by implementing additional safeguards and enhanced security measures to better protect the privacy and security of information in its systems. SRMG has also reviewed and taken steps to enhance its policies and procedures relating to the security of its systems, as well as its information life cycle management.

Additionally, in response to the incident, SRMG is providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day the change or update takes place with the bureau. SRMG is also providing you with proactive fraud assistance to help with any questions you might have or in the event you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to https://secure.identityforce.com/benefit/saco and follow the instructions provided. When prompted please provide the following unique code to receive services: . In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18. Please note when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information:

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and be prepared to supply the fraud specialist with your unique code listed within.

You are encouraged to take full advantage of these services. Enclosed you will find additional materials regarding the resources available to you, and the steps you can take to further protect your personal information.

Again, SRMG values the security of the personal data it maintains, and understand the frustration, concern, and inconvenience that this incident may have caused.

Sincerely,

Ross Emery, MD
President/Administrator

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: 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, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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) current address and any previous addresses for the past five years; and
(5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles.

The request must also include 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (https://www.transunion.com/fraud-alerts); or
- Experian (https://www.experian.com/fraud/center.html).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are listed above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.
For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and https://ag.ny.gov/.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are approximately 0 Rhode Island residents that may be impacted by this event.