



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

Gregory Bautista  
Office: (267) 930-1509  
Fax: (267) 930-4771  
Email: [gbautista@mullen.law](mailto:gbautista@mullen.law)

1127 High Ridge Road, #301  
Stamford, CT 06905

2020 AUG 11  
PM 12:47  
OFFICE OF THE ATTORNEY GENERAL

August 7, 2020

**VIA U.S. MAIL**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Event**

Dear Sir or Madam:

Our office represents Summit Medical Associates (“Summit”), located at 4656 W. Jefferson Blvd, Suite 125, Fort Wayne, IN 46804. We write on behalf of Summit to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Summit does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On or about June 5, 2020, Summit discovered that it was unable to access certain data and records stored on its server. Summit immediately launched an investigation, with the assistance of third-party forensic computer experts, to determine the nature and scope of the incident. It was determined that certain information was encrypted by ransomware. Summit’s investigation determined there was potential unauthorized access to its server between January 24, 2020 and June 5, 2020. Summit then worked to identify its patients whose personal information may have been accessible to the unauthorized actor. That process concluded July 28, 2020. Though we have no evidence the unauthorized actor actually accessed or acquired personal or protected information on Summit’s server, out of an abundance of caution, Summit is providing notice to individuals whose information may have been impacted by the event. The type of personal information related to the affected New Hampshire resident which may have been accessible to the unauthorized actor included the following: name, medical information, and Social Security number.

**Notice to New Hampshire Resident**

On or about August 7, 2020, Summit is providing written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. A sample of the letter is attached hereto and labeled as *Exhibit A*.

**Other Steps Taken and To Be Taken**

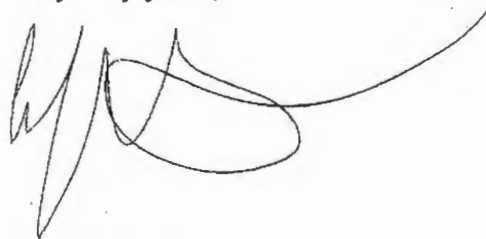
Upon discovering the event, Summit moved quickly to investigate and respond to the incident, assess the security of Summit systems, and notify potentially affected individuals. Summit is also working to implement additional safeguards and training to its employees.

Additionally, Summit is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Summit is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Summit is also reporting this matter to other regulators as required.

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-1509.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Gregory Bautista', with a long horizontal flourish extending to the right.

Gregory Bautista of  
MULLEN COUGHLIN LLC

GJB/mwj  
Enclosure

# **EXHIBIT A**

Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

**Re: Notice of Data Event**

Dear <<Name 1>>

Summit Medical Associates (“Summit”) is writing to inform you of a recent event that may impact the privacy of some of your personal information. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against potential misuse of your information, should you feel it necessary.

**What Happened?** On or about June 5, 2020, Summit discovered that it was unable to access certain data and records stored on its server. Summit immediately launched an investigation, with the assistance of third-party forensic computer experts, to determine the nature and scope of the incident. It was determined that certain information was encrypted by ransomware. Summit’s investigation determined there was potential unauthorized access to its server between January 24, 2020 and June 5, 2020. Summit then worked to identify its patients whose personal information may have been accessible to the unauthorized actor. That process concluded July 28, 2020. Though we have no evidence the unauthorized actor actually accessed or acquired personal or protected information on Summit’s server, out of an abundance of caution, Summit is notifying you because personal information related to you may have been accessible.

**What Information Was Involved?** The information potentially contained on the server at issue may have included your name, medical information, and Social Security number. We have no evidence that your information was subject to actual or attempted misuse.

**What We Are Doing.** Summit takes this incident and the security of your personal information seriously. Upon discovery, we immediately launched an investigation to determine the nature and scope of the event and to identify impacted individuals. We are reviewing our policies, procedures, and processes related to handling of and access to personal information. We will also notify the Department of Health and Human Services and other regulators of this incident as required.

**What You Can Do.** You can review the enclosed *Steps You Can Take to Protect Your Personal Information*. We also encourage you to review your financial and account statements and explanation of benefits forms and report all suspicious activity to the institution that issued the record immediately.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact our dedicated call center at 866-977-1033, 9:00 am to 9:00 pm, EST Monday through Friday, excluding major U.S. holidays. We can also be reached at 4656 W. Jefferson Blvd, Suite 125, Fort Wayne, IN 46804.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

A handwritten signature in black ink, appearing to read "B. Apuri". The signature is written in a cursive style with a large initial "B" and a long, sweeping underline.

Dr. Bhaktavatsala Apuri

## Steps You Can Take to Protect Your Personal Information

### **Monitor Your Accounts.**

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity.

### **Credit Reports.**

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

### **Security Freeze.**

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

**Experian**  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**  
P.O. Box 105788  
Atlanta, GA 30348  
1-888-298-0045  
[www.equifax.com/personal/  
credit-report-services](http://www.equifax.com/personal/credit-report-services)

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

**Experian**  
P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts)

**Equifax**  
P.O. Box 105069  
Atlanta, GA 30348  
1-888-836-6351  
[www.equifax.com/personal/  
credit-report-services](http://www.equifax.com/personal/credit-report-services)

### **Additional Information.**

You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission.

The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General.

**For Maryland residents**, the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov). **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](http://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 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; <https://ag.ny.gov/>. **For North Carolina residents**, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at [www.ncdoj.gov](http://www.ncdoj.gov). **For Rhode Island residents**, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is approximately one Rhode Island resident impacted by this incident. This notice has not been delayed by a law enforcement investigation.