



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

Paul T. McGurkin, Jr.  
Office: (267) 930-4788  
Fax: (267) 930-4771  
Email: pmcgurkin@mullen.law

426 W. Lancaster Avenue, Suite 200  
Devon, PA 19333

September 14, 2020

**VIA E-MAIL**

Office of the Attorney General  
1125 Washington Street SE  
PO Box 40100  
Olympia, WA 98504-0100  
E-mail: [securitybreach@atg.wa.gov](mailto:securitybreach@atg.wa.gov)

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Northern Light Health located at 43 Whiting Hill Road Suite 500, Brewer, Maine 04412, and are writing to notify your office of an incident that may affect the security of some personal information relating to two hundred and eighty (280) Washington residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Northern Light Health does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On July 16, 2020, Northern Light Health received notification of a cyber incident from one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”). Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to numerous philanthropical organizations in various industries, including healthcare. Blackbaud reported that in May 2020, it experienced a ransomware attack during which certain information it maintained for its customers was subject to unauthorized access between May 14, 2020 and May 20, 2020. On July 30, 2020, Northern Light Health received further information from Blackbaud that allowed it to further investigate the potentially impacted population. On September 8, 2020 Northern Light Health confirmed the identities of the potentially impacted individuals.

The information that could have been subject to unauthorized access includes name, address, phone number, date of birth, email address, gender, and the Northern Light Hospital(s) (and

possibly the department(s)) where patients received medical care, and the associated date(s) of service.

### **Notice to Washington Residents**

On September 14, 2020, Northern Light Health provided written notice of this incident to all potentially affected individuals, which includes two hundred and eighty (280) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

### **Other Steps Taken and To Be Taken**

Upon discovering the event, Northern Light Health moved quickly to investigate and respond to the incident, and notify potentially affected individuals. Northern Light Health is also re-evaluating its existing policies and procedures regarding third-party vendors and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

Additionally, Northern Light Health 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. Northern Light Health is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,




Paul T. McGurkin, Jr. of  
MULLEN COUGHLIN LLC

PTM/eeb  
Enclosure

# EXHIBIT A

  
**Northern Light  
Health.**  
Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

September 14, 2020

F7803-L01-0000001 T00001 \*\*\*\*\*OEL LINE  
SAMPLE A SAMPLE - L01 NLH - NOTIFICATION LETTER  
APT #123  
123 ANY ST  
ANYTOWN, US 12345-6789  


Dear Sample A Sample:

Northern Light Health writes to inform you of a recent incident that may affect the privacy of some of your health information. On Thursday, July 16, 2020, Northern Light Health received notification of a cyber incident from one of our third-party vendors, Blackbaud, Inc. (“Blackbaud”). Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to numerous philanthropical organizations in various industries, including healthcare. Northern Light Health, along with many other organizations around the world with charitable missions, was among the victims of this Blackbaud cyber incident. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Northern Light Health data. This notice provides information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

***What Happened?*** Blackbaud reported that in May 2020, it experienced a ransomware attack during which certain information it maintained for its customers was taken “hostage” by a cybercriminal. Blackbaud reported the incident to law enforcement and worked with forensic consultants to investigate. Following its investigation, Blackbaud notified its customers that a cybercriminal may have accessed or acquired certain Blackbaud customer data before Blackbaud locked the unknown actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, Northern Light Health immediately began to determine what, if any, sensitive Northern Light Health data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On July 30, 2020, Northern Light Health received further information from Blackbaud that allowed us to determine that the information affected included some limited protected health information.

***What Information Was Involved?*** Our investigation determined that the impacted Blackbaud systems contained your name, address, phone number, email address, date of birth, gender, the Northern Light Hospital(s) (and possibly the department(s)) where you have received medical care, and the associated date(s) of service.

***What Information Was NOT Involved?*** No credit card information or bank account information was accessed by the cybercriminal. No Acadia Hospital information was involved in this incident.

***What Has Blackbaud Done?*** Blackbaud reported that it paid the “ransom” demanded by the cybercriminal. According to Blackbaud, upon receipt of this payment this criminal stated that they deleted the copy of the data the criminal removed. Further, Blackbaud has hired an Internet expert that will continuously monitor online activity for the presence of any of the ransomed information.



***What We Are Doing.*** The confidentiality, privacy, and security of your information is among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of your information, we are working to review our existing policies and procedures regarding our third-party vendors and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We also provided the legally required notification of this incident to the United States Department of Health and Human Services.

***What You Can Do.*** We recommend you remain vigilant for attempts to obtain sensitive information from you using social engineering. This is when someone requests you provide sensitive information such as bank account information or Social Security number by using information about your recent medical visit in an attempt to show the request is legitimate. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information.

We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (877) 339-1548 between the hours of 9 am to 11 pm ET Monday - Friday and 11 am to 8 pm ET Saturday - Sunday and be prepared to reference Engagement Number DB21847. You may also write to Northern Light Health at 43 Whiting Hill Road Suite 500, Brewer, Maine 04412.

We regret the inconvenience or concern this incident may have caused.

Sincerely,

A handwritten signature in cursive script, appearing to read "Matthew Weed".

Matthew Weed  
Senior Vice President & Chief Strategy Officer

## *STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION*

### **Monitor Accounts**

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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.

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 30348-5788  
1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

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 9554  
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-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

#### **Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008

[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, 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](http://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 and your state Attorney General.

**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](http://www.riag.ri.gov); 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 487 Rhode Island residents impacted by this incident.