



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

DEC 18 2020

CONSUMER PROTECTION

Alexandria N. Murphy
Office: (267) 930-1345
Fax: (267) 930-4771
Email: amurphy@mullen.law

5133 Harding Pike, B-10, #310
Nashville, TN 37205-2891

December 9, 2020

VIA FIRST-CLASS 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:

We represent Blair Academy, located at 2 Park Street, Blairstown, NJ 07825, and write to notify your office of an incident that may affect the security of some personal information relating to twelve (12) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Blair Academy 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 July 16, 2020, Blair Academy received notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident occurring at Blackbaud. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Blair Academy. Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020.

Upon learning of the Blackbaud incident, Blair Academy immediately commenced an investigation to determine what, if any, sensitive Blair Academy data was potentially involved.

Mullen.law

While Blackbaud's initial indication was that only name and date of birth were impacted, Blair Academy worked diligently to gather further information from Blackbaud to confirm what information relating to its constituents was impacted. On or about September 29, 2020 Blair Academy first learned that additional data types may be impacted. On or about October 20, 2020, Blackbaud provided sufficient data to confirm the population of individuals with protected personal information potentially accessible within the impacted Blackbaud database. Thereafter, Blair Academy worked to identify address information to notify impacted individuals. The information that could have been subject to unauthorized access includes name, address, and Social Security number.

Notice to New Hampshire Residents

On or about December 9, 2020, Blair Academy provided written notice of this incident to affected individuals, which includes twelve (12) New Hampshire 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, Blair Academy moved quickly to work with Blackbaud to understand the results of its investigation, assess the impact on Blair Academy data, and notify potentially affected individuals. Blair Academy is also working to review 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. Blair Academy is providing access to credit monitoring services for twenty-four (24) months, through CyberScout, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

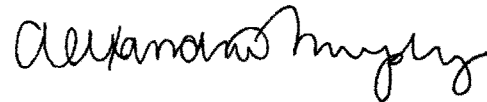
Additionally, Blair Academy is encouraging impacted individuals to remain vigilant against incidents of identity theft and fraud, to review their account statements, and to monitor their credit reports for suspicious activity. Blair Academy is also providing individuals with information on how to place 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, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Blair Academy is notifying the consumer reporting bureaus and other state regulators as required.

Office of the New Hampshire Attorney General
December 9, 2020
Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1345.

Very truly yours,

A handwritten signature in black ink, appearing to read "Alexandria N. Murphy". The signature is written in a cursive, flowing style.

Alexandria N. Murphy of
MULLEN COUGHLIN LLC

ANM/nsj

EXHIBIT A



BLAIR ACADEMY
 Return Mail Processing Center
 PO 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>>

<<VARIABLE Data 2>>

Dear <<Name1>>:

Blair Academy writes to inform you of a recent incident that may affect the privacy of some of your information. On Thursday, July 16, 2020, Blair Academy received notification from one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Blair Academy. 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 Blair Academy 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 incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, Blair Academy immediately commenced an investigation to determine what, if any, sensitive Blair Academy data was potentially involved. While Blackbaud’s initial indication was that only name and date of birth were impacted, we continued to work diligently to gather further information from Blackbaud to confirm what information relating to you was impacted. On or about September 29, 2020, Blackbaud confirmed that additional data types may have been impacted. On or about October 20, 2020 Blackbaud provided information that allowed Blair Academy to confirm the population of individuals with protected personal information potentially accessible within the impacted Blackbaud database. Thereafter, we worked to identify address information and notify those impacted.

What Information Was Involved? Our investigation determined that the impacted Blackbaud systems contained your name, address, <<Data Elements>>. Please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by the unknown actor.

What Are We Doing? The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, 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.

Blair Academy has also secured the services of CyberScout to provide you with credit monitoring and identity restoration services for twenty-four (24) months, at no cost to you. More information on how to enroll in these services can be found in the enclosed *Steps You Can Take to Help Protect Your Information*.

What You Can Do. We encourage you to enroll in the credit monitoring and identity restoration services we are offering you and to review the enclosed *Steps You Can Take to Help Protect Your Information* for more information on what you can do to help protect your personal information.

For More 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 1-800-476-0680 between the hours of 9 a.m. to 9 p.m. Eastern Time, Monday through Friday, except holidays. You may also write to Blair Academy at P.O. Box 600, Blairstown, NJ 07825.

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

Sincerely,

James Frick

James Frick, Chief Operating Officer
Blair Academy

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring and Utilize Resolution Services, if Necessary

We are providing you with access to **Single Bureau Credit Monitoring*** services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must sign up by March 27, 2021 at the latest.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please navigate to:

<https://www.cyberscouthq.com/> [REDACTED]

If prompted, please provide the following unique code to gain access to services: [REDACTED]

Once registered, you can access Monitoring Services by selecting the “Use Now” link to fully authenticate your identity and activate your services. **Please ensure you take this step to receive your alerts.** In order for you to receive the monitoring services described above, you need to sign up by **March 27, 2021 at the latest.**

Monitor Your Accounts

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 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

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

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

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, 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, 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

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289
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

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; 1-877-ID-THEFT (1-877-438-4338); and 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 District of Columbia residents, the Attorney General for the District of Columbia may be contacted at 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; (202) 727-3400; and <https://oag.dc.gov>

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 410-528-8663; and marylandattorneygeneral.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; <https://ag.ny.gov/>.

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 Rhode Island Residents, the 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 **RI #** Rhode Island residents impacted by this incident.

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 a violator. 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.