



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED
JAN 07 2021
CONSUMER PROTECTION

Julie Siebert-Johnson
Office: (267) 930-4005
Fax: (267) 930-4771
Email: jsjohnson@mullen.law

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

December 30, 2020

VIA U.S. MAIL

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

Re: Notice of Blackbaud Data Event

Dear Sir or Madam:

We represent Darlington School located at 1014 Cave Spring Rd SW, Rome, Georgia 30161, and are writing to notify your office of an incident that may affect the security of some personal information relating to three (3) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Darlington School 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 July 16, 2020, Darlington School received notification of a cyber incident from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"). Blackbaud is a cloud computing provider that provides financial services tools to organizations and schools, including Darlington School. Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Blackbaud reported that the threat actor was able to exfiltrate data from Blackbaud's network at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. While Blackbaud discovered this activity in May 2020, it was not until July 16, 2020 that Blackbaud notified Darlington School that an unknown actor may have accessed or acquired certain Blackbaud customer data. When Blackbaud first notified Darlington School of this incident, it reported that certain information, such as Social Security

Mullen.law

numbers, were encrypted within the Blackbaud systems and, therefore, were not accessible to the threat actor.

Upon receiving notice of the cyber incident, Darlington School immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Darlington School data. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident and to assess the risk to any Darlington School data stored on impacted systems.

On September 29, 2020, more than two months after first notifying Darlington School, Blackbaud notified Darlington School again, and stated that, contrary to its previous representations, certain information including Social Security numbers and Tax Identification numbers may have been subject to unauthorized access or acquisition. Blackbaud reported that at some historical point, this information was transferred into an unencrypted state without Darlington School's knowledge, and therefore this information may have been accessible to the threat actor. Darlington School immediately investigated this expanded scope to confirm the entities to whom this information related. On or about October 27, 2020, Darlington School received further information from Blackbaud about this incident and the scope of the impact to Darlington School data which aided its internal analysis. However, given that certain information specifically related to the historical, unencrypted data was not accessible to Darlington School, Darlington School was reliant upon Blackbaud to provide the information that was present on Blackbaud's network at the time of the incident. Based on additional information received from Blackbaud, on December 4, 2020, Darlington School confirmed the population of individuals whose information was potentially subject to unauthorized acquisition. Darlington School thereafter worked to provide notice to potentially impacted individuals as quickly as possible.

The information potentially subject to unauthorized acquisition included name, Social Security number, and financial account information.

Notice to New Hampshire Residents

On December 30, 2020, Darlington School provided written notice of the Blackbaud incident to three (3) New Hampshire residents. Written notice was 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, Darlington School moved quickly to obtain information from Blackbaud regarding their incident. Darlington School then provided notice to potentially affected individuals associated with Darlington School. Darlington School is working to review 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. Further, Darlington School is also providing access to identity monitoring services for 24 months through either CyberScout or Epiq to individuals whose personal information was potentially affected by this incident at no cost to these individuals. To date, Darlington School has not received any

information from Blackbaud that any Darlington School information was specifically accessed or acquired as a result of this event.

Additionally, Darlington School is providing notified individuals with guidance on how to better protect against identity theft and fraud. Darlington School is providing individuals with 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. Darlington School will also be notifying other state 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) 930-4005.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Julie Siebert-Johnson', written in a cursive style.

Julie Siebert-Johnson of
MULLEN COUGHLIN LLC

JSJ/acl
Enclosure

EXHIBIT A

DATE

[First Name] [Middle Name] [Last Name] [Suffix]

[Address Line 1]

Address Line 2

[City, State Zip]

Re: Notice of Data [variable field]

Dear [First Name] [Last Name] [Suffix]:

Darlington School writes to make you aware of a recent incident involving one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”), that may affect the privacy of some of your information. While, to date, we have no evidence of any actual or attempted misuse of any information as a result of this incident, this notice provides information about the Blackbaud incident, our response and efforts to obtain additional information from Blackbaud, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On Thursday July 16, 2020, Darlington School received notification from Blackbaud of a cyber incident on its network. Blackbaud is a cloud computing provider that provides financial services tools to organizations and schools, including Darlington School. 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. Blackbaud reported that the threat actor was able to exfiltrate data from Blackbaud’s network at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. While Blackbaud discovered this activity in May 2020, it was not until July 16, 2020, that Blackbaud notified Darlington School that an unknown actor may have accessed or acquired certain Blackbaud customer data. When Blackbaud first notified Darlington School of this incident, it reported that certain information, such as Social Security numbers, were encrypted within the Blackbaud systems and, therefore, were not accessible to the threat actor.

Upon receiving notice of the cyber incident, Darlington School immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Darlington School data. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident and to assess the risk to any Darlington School data stored on impacted systems.

On September 29, 2020, more than two months after first notifying Darlington School, Blackbaud notified Darlington School again, and stated that, contrary to its previous representations, certain Tax Identification numbers may have been subject to unauthorized access or acquisition. Blackbaud reported that at some historical point, certain Taxpayer Identification numbers were transferred into an unencrypted state without Darlington School’s knowledge, and this information may have been accessible to the threat actor. Darlington School immediately investigated this expanded scope to confirm the entities to whom this information related. On or about October 27, 2020, Darlington School received further information from Blackbaud about this incident and the scope of the impact to Darlington School data which aided our internal analysis. However, given that certain information specifically related to the historical, unencrypted data was not accessible to Darlington School, we were reliant upon Blackbaud to provide the information that was present on Blackbaud’s network at the time of the incident. On December 4, 2020, Darlington School received additional information from Blackbaud which allowed it

to confirm the population of individuals whose information was potentially subject to unauthorized acquisition. We thereafter worked to provide notice as quickly as possible.

What Information Was Involved? Our investigation determined that the involved Blackbaud systems contained your name and [impacted 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 We Are 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. We will also be notifying regulators, as required.

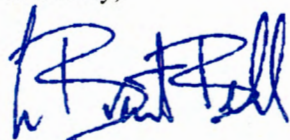
As an added precaution, and at no cost to you, we are providing you with access to identity monitoring services provided by CyberScout for 24 months. Please review the enclosed *Steps You Can Take to Help Protect Your Information* for additional information and enrollment instructions.

What You Can Do. 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 and to detect errors. Please 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, as well as information on how to enroll in the credit monitoring services being offered.

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 us at (706) 802-4390, Monday through Friday, between the hours of 9 a.m. and 3 p.m. Eastern Time. Additionally, you may also write to Darlington School at datasupport@darlingtonschool.org.

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

Sincerely,



Brent Bell
Head of School
Darlington School

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Identity Monitoring

- **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 must enroll within 90 days from the date of this letter.

ADDITIONAL INFORMATION REGARDING YOUR 24-MONTH MONITORING PRODUCT

Proactive Fraud Assistance. For sensitive breaches focused on customer retention, reputation management, or escalation handling, CyberScout provides unlimited access during the service period to a fraud specialist who will work with enrolled notification recipients on a one-on-one basis, answering any questions or concerns that they may have. Proactive Fraud Assistance includes the following features:

- Fraud specialist-assisted placement of fraud alert, protective registration, or geographical equivalent, in situations where it is warranted.
- After placement of a Fraud Alert, a credit report from each of the three (3) credit bureaus is made available to the notification recipient (United States only).
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Answering any questions individuals may have about fraud.
- Provide individuals with the ability to receive electronic education and alerts through email. (Note that these emails may not be specific to the recipient’s jurisdiction/location.)

Identity Theft and Fraud Resolution Services. Resolution services are provided for enrolled notification recipients who fall victim to an identity theft as a result of the applicable breach incident. ID Theft and Fraud Resolution includes, but is not limited to, the following features:

- Unlimited access during the service period to a personal fraud specialist via a toll-free number.
- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparation of all documents needed for credit grantor notification, and fraud information removal purposes.
- All phone calls needed for credit grantor notification, and fraud information removal purposes.
- Notification to any relevant government and private agencies.
- Assistance with filing a law enforcement report.
- Comprehensive case file creation for insurance and law enforcement.
- Assistance with enrollment in applicable Identity Theft Passport Programs in states where it is available and in situations where it is warranted (United States only).
- Assistance with placement of credit file freezes in states where it is available and in situations where it is warranted (United States only); this is limited to online-based credit freeze assistance.
- Customer service support for individuals when enrolling in monitoring products, if applicable.

- Assistance with review of credit reports for possible fraudulent activity.

Unlimited access to educational fraud information and threat alerts. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Monitor Accounts

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, 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 one-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

TransUnion

P.O. Box 2000

Equifax

P.O. Box 105069

Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

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. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General can be contacted at 441 4th St. NW #1100 Washington, D.C. 20001; by phone at 202-727-3400; and by email at oag@dc.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act ("FCRA"). Those rights include but are not limited to 1) the right to be told if information in your credit file has been used against you; 2) the right to know what is in your credit file 3) the right to ask for your credit score; and 4) and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting agencies must 1) correct or delete inaccurate, incomplete, or unverifiable information; and 2) limit access to your file; and 3) get your consent for credit reports to be provided to employers. Additionally, consumer reporting agencies may 1) not report outdated negative information; and 2) limit "prescreened" offers of credit and insurance you receive based on information in your credit report. You may also 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 <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.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 can 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 1-919-716-6000; www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island Residents, the Rhode Island Attorney General can be contacted at 150 South Main Street, Providence, RI 02903; 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 approximately 4 Rhode Island residents impacted by this incident.