



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

STATE OF NH  
DEPT OF JUSTICE  
2020 NOV 16 PM 3:16

M. Alexandra Belton  
Office: (267) 930-4773  
Fax: (267) 930-4771  
Email: [abelton@mullen.law](mailto:abelton@mullen.law)

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

November 11, 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:

We represent Forsyth Country Day School (“FCDS”) located at 5501 Shallowford Road, Lewisville, North Carolina 27023 and write to notify your Office of an incident that may affect the security of some personal information relating to approximately one (1) New Hampshire resident. This notice may be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, FCDS 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**

In July 2020, Blackbaud reported that it experienced a ransomware incident in May 2020 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 certain data was acquired by the threat actor at some point before Blackbaud locked the threat actor out of the system on May 20, 2020.

Blackbaud initially reported that credit card information, financial account information, and Social Security numbers were not affected by the ransomware event; however, on September 29, 2020, Blackbaud notified FCDS that its previous statement was incorrect, and some such data was potentially affected by the incident. FCDS immediately took steps and worked with Blackbaud to obtain additional information surrounding this data. On October 9, 2020, Blackbaud provided FCDS with information that allowed it to determine what specific FCDS data was potentially affected. FCDS then worked diligently to identify those individuals and their appropriate contact information in order to provide notice of this incident. On or around November 4, 2020, FCDS confirmed that this information included information for approximately

[Mullen.law](http://Mullen.law)

November 11, 2020

Page 2

one (1) New Hampshire resident. The type of information potentially impacted for the New Hampshire resident includes name and Social Security number.

#### **Notice to New Hampshire Resident**

On November 10, 2020, FCDS provided written notice of this incident to affected individuals, which includes approximately one (1) New Hampshire resident. 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, FCDS moved quickly to investigate and respond to the incident and to notify potentially affected individuals. This included coordination with Blackbaud to confirm what information may have been affected by Blackbaud's incident. FCDS is reviewing 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, through Blackbaud, FCDS is providing potentially impacted individuals access to credit monitoring services for 24 months. FCDS is also providing individuals with guidance on how to better protect against identity theft and fraud, including 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. FCDS is also notifying 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) 930-4773.

Very truly yours,



M. Alexandra Belton of  
MULLEN COUGHLIN LLC

MABB/jcl  
Enclosure

# EXHIBIT A



Forsyth  
For What's Ahead

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

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

<<Date>>

Dear <<Salutation>>:

Forsyth Country Day School ("FCDS") writes to make you aware of a recent incident that may affect the privacy of some of your information. FCDS 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 FCDS. 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 FCDS 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?** In July, Blackbaud reported that it experienced a ransomware incident in May 2020 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 certain data was acquired by the threat actor at some point before Blackbaud locked the threat actor out of the system on May 20, 2020.

Blackbaud initially reported that credit card information, financial account information, and Social Security numbers were not affected by the ransomware event; however, on September 29, 2020, Blackbaud notified us that its previous statement was incorrect and some such data was potentially affected by the incident. FCDS immediately took steps and worked with Blackbaud to obtain additional information surrounding this data. On October 9, 2020, Blackbaud provided us with information that allowed us to determine what specific FCDS data was potentially affected. We then worked diligently to identify those individuals and their appropriate contact information in order to provide notice of this incident.

**What Information was Involved?** Based on the information received from Blackbaud, our investigation determined that the involved Blackbaud systems contained your name and <<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, nor has Blackbaud reported any actual or attempted misuse of FCDS information.

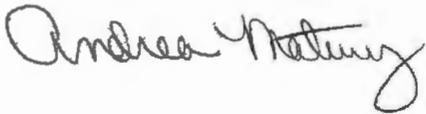
**What We Are Doing?** The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures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

**What You Can Do?** We encourage you to remain vigilant against incidents of fraud or identity theft and to monitor your accounts and free credit reports for suspicious activity and to detect errors. Please also review the enclosed "Steps You Can Take to Help Protect Your Information."

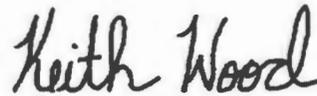
Although Blackbaud has not reported, and our internal investigation has not found, any actual or attempted misuse of your information as a result of this event, Blackbaud is offering credit monitoring services for twenty-four (24) months at no cost to you as an added precaution. A description of services and instructions on how to enroll can be found within the enclosed "Steps You Can Take to Help Protect Your Information." Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

**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 contact us at 855-914-4673, available Monday through Friday, from 9:00 a.m. to 9:00 p.m., Eastern Time. You may also write to FCDS at 5501 Shallowford Road, Lewisville, North Carolina 27023. We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,



Andrea Matney  
Associate Head of School for Finance and Operations  
Forsyth Country Day School



Keith Wood  
Director of Information Technology  
Forsyth Country Day School

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### Enroll in Credit Monitoring

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

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

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.

### Monitor Accounts

Under U.S. law you are entitled to one (1) free credit report annually from each of the three (3) 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)

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 (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 19106  
1-800-680-7289  
[www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-766-0008  
[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. This notice has not been delayed by law enforcement.

*For Maryland residents*, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; or [www.oag.state.md.us](http://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](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 can be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <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; or [www.ncdoj.gov](http://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, Rhode Island 02903; 1-401-274-4400; or [www.riag.ri.gov](http://www.riag.ri.gov). Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 4 Rhode Island residents impacted by this incident.

*For Washington, D.C. residents*, the Office of Attorney General for the District of Columbia can be reached at: 441 4<sup>th</sup> Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; or <https://oag.dc.gov>.