Alexander T. Walker
Office: (267) 930-4801
Fax: (267) 930-4771
Email: awalker@mullen.law

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

August 31, 2020

VIA E-MAIL

Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent The Open Window School ("OWS") located at 6128 168th Place SE, Bellevue, WA 98006, and write to notify your office of an incident that may affect the security of some personal information relating to one thousand nine hundred twenty-nine (1,929) Washington residents. This notice may be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, OWS 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, OWS received a communication 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 OWS. Upon receiving notice of the cyber incident, OWS immediately commenced an investigation to better understand the nature and scope of the incident and any impact on OWS data. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On or about August 6, 2020, OWS received further information from Blackbaud that allowed it to ascertain the scope of the breach and confirm the information potentially affected may have contained personal information.

In its initial communication, 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 understand what occurred. 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. Based on

OWS's investigation, it was determined that the information that could have been subject to unauthorized access or acquisition includes individuals' name, date of birth, or medical information, although that information may vary by individual. OWS does not store Social Security numbers or bank or credit card information in the impacted Blackbaud systems.

Notice to Washington Residents

On August 31, 2020, OWS began providing written notice of this incident to affected individuals, which include one thousand nine hundred twenty-nine (1,929) 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, OWS moved quickly to investigate and respond to the incident and to notify potentially affected individuals. This included extensive coordination with Blackbaud to ascertain the scope of the breach and confirm what information could have been potentially affected that may have contained personal information. OWS 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.

Additionally, OWS 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. OWS 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4801.

Very truly yours,

Alexander Walker of
MULLEN COUGHLIN LLC

ATW:zlg
Enclosure

EXHIBIT A

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

<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

August 31, 2020

Re: Notice of Data Breach

Dear <<Name 1>>:

Open Window School ("OWS") writes to inform you of a recent incident that may affect the privacy of some of your information. On Thursday, July 16, 2020, OWS received notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), regarding a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including OWS. 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 OWS data. This notice provides information about the Blackbaud incident, our response, and what information may have been accessed during this incident.

What Happened? Blackbaud reported that in May 2020, it experienced a ransomware incident that resulted in an unknown actor's encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to investigate. Blackbaud reports that the data accessed by the cybercriminal was destroyed and, based on the nature of the incident, Blackbaud's research, and law enforcement's investigation, they have no reason to believe the data will be misused or disseminated. Following its investigation, Blackbaud notified its customer organizations, including OWS, that an unknown actor may have accessed or acquired certain Blackbaud customer data. They are not able to confirm for certain whether any data relating to OWS was actually accessed or acquired.

Upon receiving initial notification of the Blackbaud incident, OWS immediately began to determine what, if any, sensitive OWS data was potentially involved. This investigation included working diligently to gather further information and technical support from Blackbaud to understand the scope of the incident.

What information was involved? OWS does not store Social Security numbers and bank or credit card information in the impacted Blackbaud systems; therefore this information was not compromised. Further, Blackbaud has indicated that the cybercriminal did not gain access to usernames and passwords because those field were encrypted. The types of personal information stored in the potentially impacted Blackbaud systems at the time of the incident include your <<Breached Elements>>. To reiterate what we said above, Blackbaud has no reason to believe any data accessed by the cybercriminal has been or will be misused or disseminated.

For More Information. We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions or need assistance, please call our dedicated assistance line at 1-855-917-3592 between the hours of 6:00 am PT and 6:00 pm PT. You can also write to OWS at Attn: Head of School, Open Window School, 6128 168th Place S.E. Bellevue, WA 98006.

We sincerely regret the inconvenience this event may cause you. 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.

Sincerely,

Open Window School

Steps You Can Take to Help Protect Your Information

Monitor Your 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 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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	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); 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.