January 22, 2021

Anjali C Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Submission

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Data Security Incident

Dear Attorney General Frey:

We represent Oldfields School ("Oldfields") with respect to a potential data security incident involving Blackbaud, Inc. ("Blackbaud") described in more detail below. Oldfields is a private college preparatory school for girls, and is located at 1500 Glencoe Road, Sparks Glencoe, Maryland. Oldfields does not have any evidence of the misuse of any information. Oldfields takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. **Nature of the security incident.**

Blackbaud is a cloud computing provider that is used by Oldfields and many other charitable organizations to organize and store donor information. In July 2020, as you may already be aware, Blackbaud notified hundreds of charitable organizations, including Oldfields, that they experienced a cybersecurity incident which resulted in the exposure of personal information maintained by clients on their platform. Oldfields was first notified of this incident by Blackbaud July 16, 2020.

On September 30, 2020, Oldfields was notified by Blackbaud that scanned documents, consisting of Oldfields' constituents' records, were not encrypted. Based on Oldfields' internal investigation, it appears that some personal information was compromised, specifically a scanned copy of a check.

2. **Number of Maine residents affected.**

A total of six (6) residents of Maine may have been potentially affected by this incident. Notification letters were mailed on January 22, 2021, by first class mail. A sample copy of the notification letter is included with this letter.

3. **Steps taken.**

Oldfields is committed to ensuring the security of all personal information in our control, and we are taking steps to prevent a similar event from occurring in the future. Blackbaud has indicated that it has taken (or plans to take) the following steps to strengthen its cybersecurity post-attack: hardening Blackbaud's

environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms; steps to improve to the granularity of reporting at both the host and network level to ensure intrusion detection capabilities; accelerating efforts to add multi-factor authentication to all of Blackbaud's self-hosted solutions; ensuring all users reset their passwords regularly; requiring stronger user passwords for certain customers; increasing efforts to migrate customers to Cloud environments (including Microsoft Azure and Amazon Web Services). Oldfields is also providing potentially impacted individuals with identity theft protection and credit monitoring services for a period of twelve (12) months at no cost through ID Experts.

4. Contact information

Oldfields remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@wilsonelser.com or (312) 821-6164.

Very truly yours,

WILSON, ELSER, MOSKOWITZ, EDELMAN & DICKER LLP

Anjali C. Das

Established 1867
OLDFIELDS
SCHOOL

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January 22, 2021

Dear <<FirstName>>,

We are writing to inform you of a data security incident involving one of our vendors, Blackbaud, Inc., ("Blackbaud") and constituent information from our databases. Blackbaud's cloud-computing services are used by Oldfields and many other schools and charitable organizations to manage, organize, and store information related to members of their community. Oldfields School takes the security of your personal information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains information about the incident and steps you can take to protect your information.

What happened:
On July 16, 2020, Blackbaud notified hundreds of educational institutions, including Oldfields, that Blackbaud was the victim of a ransomware cybersecurity incident. Since then, Oldfields has engaged and worked with outside counsel to further investigate the extent of the breach and its impact on our community.

What information was involved:
On September 30, 2020, Oldfields was notified by Blackbaud that scanned documents in our constituent records were not encrypted. After an internal audit, it was determined that your record was among a small fraction of constituent records that included a scanned copy of a check, which may have been exposed as a result of this incident. At this time, based on the information we have received from Blackbaud, we have no reason to believe that any of your personal information has been misused. However, for purposes of full disclosure, we feel it is important to inform you that your personal information may have been viewed by unauthorized individuals as a result of this incident.

What are we doing, and what you can do:
Oldfields has secured the services of IDX to provide identity-monitoring services at no cost to you, for <<12/24>> months. While we do not have any evidence of the misuse of your information, we are nonetheless notifying you out of an abundance of caution. Information about the services being provided by IDX is included in this letter.

Additionally, Blackbaud has indicated that it has taken (or plans to take) the following steps to strengthen its cybersecurity post-attack: hardening Blackbaud's environment through enhancements to access management, network segmentation, and deployment of additional endpoint and network-based platforms; steps to improve to the granularity of reporting at both the host and network level to ensure intrusion detection capabilities; accelerating efforts to add multi-factor authentication to all of Blackbaud's self-hosted solutions; ensuring all users reset their passwords regularly; requiring stronger user passwords for certain customers; increasing efforts to migrate customers to Cloud environments (including Microsoft Azure and Amazon Web Services).

Other important information:
Oldfields School values the privacy of our community and the protection of your information is a top priority. We apologize for any concern the Blackbaud data breach may cause you. If you have questions, please do not hesitate to call (800) 939-4170, Monday – Friday, 9:00 AM to 9:00 PM, EST.

Sincerely,

Bryan Engle
Director of Finance and Business Operations

IDX Enrollment

Website and Enrollment. Please visit https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code included with this letter.

Activate the monitoring provided as part of your IDX membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Telephone. Contact IDX at (800) 939-4170 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

This IDX enrollment will include one-year enrollment into:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN^{TM} MONITORING - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY– IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned ID Care Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Maryland, Rhode Island, Illinois, New York* and *North Carolina:* You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of *District of Columbia*: Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001 (202) 442-9828 https://oag.dc.gov/consumer-protection

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.freeze.equifax.com	www.experian.com/freeze	freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.