Shorecrest | Be More

Return Mail Processing Center
P.O. 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>>

RE: Notice of Data Breach

Dear <<Name 1>>:

Shorecrest Preparatory School ("Shorecrest") writes to inform you of a data privacy event experienced by one of our vendors which may impact the security of your information.

Blackbaud, Inc. ("Blackbaud") is a leading cloud computing provider which offers financial reporting and institutional advancement management tools to private academic institutions and non-profit organizations around the world, including Shorecrest. This notice provides information about Blackbaud's recent 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? On Thursday, July 16, 2020, Shorecrest received notification from one of its third-party vendors, Blackbaud, of a cyber incident. 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 consultants to investigate. Following its investigation, Blackbaud notified its customers, including Shorecrest, 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. When Blackbaud first notified Shorecrest of this incident, it reported that certain information, such as Social Security numbers, were encrypted within the Blackbaud systems and, therefore, this information was not accessible to the threat actor. Shorecrest relied on these assertions to assure certain members of its community in August 2020 that this information had not been impacted by the Blackbaud incident. Upon receiving notice of Blackbaud's cyber incident, we immediately commenced an investigation to determine what, if any, sensitive Shorecrest data was potentially involved. This investigation included working diligently with an outside incident response partner to gather further information from Blackbaud to understand the scope of the incident.

On September 29, 2020, more than two months after first notifying Shorecrest, Blackbaud notified Shorecrest again, and stated that, contrary to its previous representations, certain personal information may have been subject to unauthorized access or acquisition. While Shorecrest has not used the affected Blackbaud product in several years, Blackbaud reported that at some historical point, personal information had been transferred into an unencrypted state without Shorecrest's knowledge and this information may have been accessible to the threat actor. Because this information was not accessible to Shorecrest, we were reliant upon Blackbaud to provide the list of individuals whose unencrypted personal information was present on Blackbaud's network at the time of the incident. On October 27, 2020, Blackbaud provided this updated information, at which time we confirmed your personal information was among the data that may have been impacted.

What Information Was Involved? Our investigation determined that the involved Blackbaud systems contained your full name as well as your <<insert data elements>>. Please note that, to date, we have not received any information from Blackbaud that your information was specifically accessed or acquired by the unknown actor, but this possibility could not be ruled out.

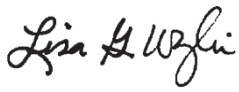
What Are We Doing? The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures 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. We will also be notifying state regulators, as required. Additionally, while we are unaware of any actual or attempted misuse of your information, in an abundance of caution, we are notifying potentially impacted individuals, including you, so that you may take further steps to protect your information, should you feel it appropriate to do so, and providing you with access to 24 months of Identity Monitoring services through CyberScout at no cost to you.

What Can You Do? We encourage you to 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 and more information on the identity monitoring services Shorecrest is offering and how to enroll.

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 800-588-1676, Monday through Friday between the hours of 9am and 9pm, Eastern Time (excluding holidays). You may also contact Shorecrest Preparatory School via email at cyberincident@shorecrest.org.

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

Sincerely,



Lisa Wylie, CPA
Chief Financial Officer
Shorecrest Preparatory School

Steps You Can Take to Help Protect Your Information

Complimentary Credit Monitoring Services

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 that 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 enroll by March 27, 2021.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please navigate to **https://cyberscouthq.com/epiq263** and, when prompted, please provide the following unique code to gain access to services: **263HQ845**. 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.

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 3 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 3 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 5 years, provide the addresses where you have lived over the prior 5 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.); and
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 7 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.

For District of Columbia residents, the Office of the District of Columbia Attorney General can be contacted at 400 6th Street, NW, Washington, DC 20001; Phone (202) 727-3400; Fax: (202) 347-8922; TTY: (202) 727-3400; Email: oag@dc.gov; or you may visit the website of the Office of the District of Columbia Attorney General at https://oag.dc.gov/.

For Kentucky Residents, the Office of the Attorney General of Kentucky can be contacted at 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601; www.ag.ky.gov; and by telephone at 1-502-696-5300.

For Maryland residents, the Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; or 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 or by writing to 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 may 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 may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www.ncdoj.gov.

Oregon residents, the Oregon Department of Justice can be contacted at, 1162 Court Street NE, Salem, OR 97301-4096; http://www.doj.state.or.us; or 877-877-9392.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; or 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 0 Rhode Island resident(s) impacted by this incident.