

Exhibit 1

We represent Shorecrest Preparatory School (“Shorecrest”), located at 5101 1st St NE, St. Petersburg, FL 33703. Shorecrest writes to notify your office of an incident that may impact the privacy of personal information relating to three (3) Maine residents. Shorecrest reserves the right to supplement this notice with new significant facts learned subsequent to its submission. By providing this notice, Shorecrest does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On Thursday, July 16, 2020, Shorecrest received notification from one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”), of a cyber incident. Blackbaud is a cloud computing provider that offers financial reporting and institutional advancement management tool to private academic institutions and non-profit organizations around the world, including Shorecrest.

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. Upon learning of the Blackbaud incident, Shorecrest immediately commenced an investigation to determine what, if any, sensitive Shorecrest data was potentially involved. This investigation included working diligently 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, Shorecrest was 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 Shorecrest confirmed personal information was among the data that may have been impacted.

The investigation determined that, in addition to first and last names, the involved Blackbaud systems potentially contained Social Security Numbers for three (3) Maine residents(s). To date, the investigation has found no evidence of any actual or attempted misuse of personal information as a result of this event.

Notice to Maine Residents

On January 26, 2021, Shorecrest began providing written notice of this incident to potentially affected individuals. This includes approximately three (3) Maine residents whose personal information as defined by Maine may have been accessible. Written notice to the individuals is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon learning of this incident, Shorecrest moved quickly to assess the security of its potentially affected data and to notify potentially impacted individuals. Shorecrest is also offering complimentary access to twenty-four (24) months of credit and identity monitoring services, including identity restoration services through CyberScout for affected individuals, and the contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident.

Additionally, Shorecrest is providing affected individuals with guidance on how to better protect themselves against identity theft and fraud. This guidance includes 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 about incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, the respective state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Shorecrest is also providing notice of this event to other relevant state regulators as required.

Exhibit A

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 some of your company’s 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 company’s 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 sensitive 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, sensitive Shorecrest 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/entities whose unencrypted 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 company’s information was among the data that may have been impacted.

What Information Was Involved? Our investigation determined that the involved Blackbaud systems contained your company’s name as well as its tax identification number. Please note that, to date, we have not received any information from Blackbaud that your company’s 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 company's information, in an abundance of caution, we are notifying our potentially impacted vendors, including you, so that you may take further steps to protect your company's information, should you feel it appropriate to do so.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your business account statements and monitoring your business credit reports for suspicious activity. You may also contact the three major credit bureaus for businesses directly to request a copy of your business credit report:

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-800-685-5000
<https://www.equifax.com/business/small-business/>

Corporate Experian

P.O. Box 2002
Allen, TX 75013
1-800-303-1640
<https://www.experian.com/small-business/corporate-credit.jsp>

Dun & Bradstreet

103 JFK Parkway
Short Hills, NJ 07078
1-844-237-6687
<https://www.dandb.com/>

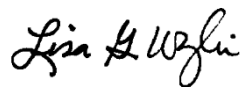
You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania 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 encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General.

The North Carolina 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 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