Appendix

Emma Willard School (the "School") is a private school in Troy, New York. This notice is based on the information currently known to the School. By providing this notice, the School does not waive any rights or defenses it may have regarding the applicability of Maine law and regulations to this incident.

Description of the Security Incident

In May 2020, Blackbaud, Inc. (a company that provides data hosting and other services to the School) experienced a data security incident. Blackbaud first notified the School (and other customers) of the incident on or about July 16, 2020. At the time of this first notice, Blackbaud informed the School that social security numbers had not been compromised, because Blackbaud stored social security numbers in encrypted format. Blackbaud also informed the School that there was little risk to any individual, because Blackbaud had paid a ransom to have stolen information deleted and had hired security experts to monitor the "dark web" to ensure the information was not being offered for sale or re-distributed.

On September 29, 2020, Blackbaud informed the School that based on further investigation, Blackbaud had determined that social security numbers of some individuals may have been stored in unencrypted format. The School requested that Blackbaud provide additional information to allow the School to validate Blackbaud's conclusion and identify individuals whose social security numbers may have been access or disclosed.

On October 20, 2020, the School received data files confirming that there was reason to believe that social security numbers, including the social security numbers of Maine residents, potentially had been accessed and/or downloaded by an unauthorized third party.

Notice to Maine Residents

The School is providing notice to individuals whose social security numbers may have been accessed and/or downloaded, including notice to sixteen (16) Maine residents. A notice in substantially the same form as the letter attached to this Appendix is being sent by mail to potentially affected Maine residents on October 28, 2020.

Other Steps Taken (or To Be Taken)

Blackbaud has informed the School that it has taken steps to address the cause of the original security incident. Blackbaud also has informed the School that it is taking steps to delete all files containing unencrypted social security numbers. In addition, as noted above, Blackbaud has informed the School that it has taken steps to mitigate any harm from the original breach, including paying a ransom in exchange for a promise to delete the stolen data files and retention of cybersecurity experts to monitor the "dark web" to ensure that the stolen data is not being offered for sale or otherwise distributed.

Although the School continues to believe the risk of this incident is low and that there is no reason to believe that the social security number of any person has or will be misused as a result of this incident, affected individuals (including Maine residents) are being offered twenty-four (24) months of free identity monitoring and fraud resolution services, as described in the attached template notice.

Finally, the School is providing potentially affected individuals with additional information on how to protect themselves against identity theft and fraud, including advising them to report any suspected incidents of identity theft or fraud to their financial institutions. The School also is providing potentially affected individuals with information on how to place fraud alerts and security freezes on their credit files, contact information for national consumer reporting agencies, and other relevant information.

Maine Resident Notice Template

October 28, 2020

[addressee]
[address line 1]
[address line 2]
[city], [state], [postal code]

Dear [first name],

We recently learned your social security number may have been disclosed in a cyberattack affecting Blackbaud, which supplies data services to Emma Willard and other schools and nonprofits worldwide.

What Happened?

In July 2020, we received notice that Blackbaud had suffered a cyberattack in May 2020 affecting personal information of some of our community members. In that first notice, Blackbaud informed us that no social security numbers were compromised, because social security numbers were stored in encrypted format. Blackbaud also informed us that there was little overall risk from this incident, because it had paid a ransom to have all stolen information deleted and had hired security experts to monitor the "dark web" to ensure the information was not being offered for sale or distributed to others.

What Information Was Involved?

Blackbaud continued its investigation and discovered some data files containing social security numbers in unencrypted format. On September 29, 2020, Blackbaud notified us that social security numbers of some Emma Willard community members potentially had been stored by Blackbaud in unencrypted format. We conducted our own investigation and, on October 20, 2020, confirmed that your social security number likely was among those stored by Blackbaud in unencrypted format.

What You Can Do.

Although we still believe the risk to you is low and we have no evidence that any of the data stolen has been sold or re-distributed, Blackbaud has arranged for you to receive free identity monitoring and fraud resolution services for 24 months. These services are described in the attached information packet and include credit monitoring, proactive fraud assistance and identity theft and fraud resolution services. The attached information packet also includes information on other resources and steps you can take to protect yourself in addition to the services offered by Blackbaud.

What We Are Doing.

Blackbaud has informed us that it has fixed the cause of this incident and taken other steps to better protect your data, including improving the overall security and monitoring of its systems.

For More Information.

We understand that this situation is frustrating and that you may have questions regarding this incident. If you have any questions or concerns, please do not hesitate to contact our Data Protection Officer, Judith Curry, at dpo@emmawillard.org or (518) 833-1316 at your earliest convenience.

Sincerely,

Virginia Arbour, CFO

Free Identity Monitoring and Fraud Resolution Services

Blackbaud is 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 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. If you become a victim of fraud, you will also have access to remediation support from a CyberScout Fraud Investigator. **To receive the monitoring service described above, you must enroll within 90 days from the date of this letter**.

Proactive Fraud Assistance. CyberScout provides unlimited access during the service period to a fraud specialist who will work with enrolled notification recipients on a one-on-one basis, answering any questions or concerns that they may have. Proactive Fraud Assistance also includes the following features:

- Placement of fraud alert, protective registration, or equivalent notices where warranted.
- After placement of a Fraud Alert, a credit report from each of the three (3) credit bureaus is made available to the notification recipient (United States only).
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Providing individuals with electronic education and alerts through email.

Identity Theft and Fraud Resolution Services. Resolution services are provided for enrolled notification recipients who fall victim to an identity theft as a result of the applicable breach incident. Identity Theft and Fraud Resolution includes, but is not limited to, the following features:

- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparing documents for credit grantor notification, and fraud information removal purposes.
- Phone calls needed for credit grantor notification, and fraud information removal purposes.
- Notification to relevant government and private agencies.
- Assistance with filing a law enforcement report.
- Comprehensive case file creation for insurance and law enforcement.
- Assistance with enrollment in applicable Identity Theft Passport Programs in states where it is available and in situations where it is warranted (United States only).
- Assistance with placement of online-based credit file freezes in states where it is available and in situations where it is warranted (United States only).
- Unlimited access to educational fraud information and threat alerts.

How do I enroll for the free services?

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

[CREDIT MONITORING LINK]

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

[CREDIT MONITORING CODE]

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.**

To receive the services described above, you must enroll within 90 days from the date of this letter.

Self-Help Steps You Can Take to Protect Your Personal Information

Whether or not you choose to use the identity monitoring and fraud resolution services offered by Blackbaud, there are many steps you can take to protect yourself.

When dealing with a potential data security incident, you should remain vigilant by reviewing your account statements and credit reports. If you detect suspicious activity, you should promptly notify the financial institution or company that maintains the account. You also should promptly report any fraudulent activity or suspected identity theft to proper law enforcement authorities, your State Attorney General, and/or the Federal Trade Commission.

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting: https://www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by mailing an annual credit report request form to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. In addition, until April 2021, all three major credit reporting agencies are offering free weekly credit monitoring reports. You can find a copy of the request form at: https://www.annualcreditreport.com.

You may also wish to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three major reporting agencies: TransUnion, by visiting https://www.transunion.com/fraud-alerts, calling 1-800-680-7289, or mailing to P.O. Box 2000, Chester, PA 19016; Experian, by visiting https://www.experian.com/fraud/center.html, calling 1-888-397-3742, or mailing to P.O. Box 9554, Allen, TX 75013; and Equifax, by visiting https://www.equifax.com/personal/credit-report-services/, calling 1-888-766-0008, or mailing to P.O. Box 740256, Atlanta, GA 30374. Ask the company to put a fraud alert on your credit line and confirm that the company you called will contact the other two. Additional information is available at: https://www.annualcreditreport.com.

You also have a right to place a credit freeze on your credit file, which will prohibit a consumer credit reporting agency from accessing or releasing information in your credit report without your express consent. It will also prevent new credit from being opened in your name without the use of a PIN number that is issued to you. However, using a credit freeze may delay or interfere with your ability to obtain credit. Credit freezes are free of charge and will last until temporary lifted or permanently removed. To place a credit freeze, please contact each major reporting agency listed above.

For additional information on how to avoid identity theft, the Federal Trade Commission provides a comprehensive guide to help you guard against, identify, and respond to identity theft, a copy of which may be found at: https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf. For more information, please visit https://www.identitytheft.gov, call 1-877-ID-THEFT (1-877-438-4338), or send mail to Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.