Wildwood School

<<Date>> (Format: Month Day, Year)

Parent or Guardian of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

NOTICE OF DATA BREACH

Dear Parent or Guardian of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We have recently learned that our third-party fundraising software provider, Blackbaud, experienced a global data security breach earlier this year, impacting many of its clients around the world, including Wildwood School. Unfortunately, this incident involves the potential exposure of personal information of some of our community members.

The compromised data did not contain any credit card information or other personally identifiable information such as bank account information, usernames, passwords, or Social Security numbers.

While the cyber-attack did not occur at Wildwood School or as a result of any action on our part, we take the protection of our community's information very seriously and wanted to make you aware of the incident, what it may mean to you, and steps you can take to secure your child's information.

What Happened? Blackbaud is a software service provider used by non-profit companies, schools, and institutions. Earlier this year, Blackbaud was the subject of a ransomware attack, and the cyber-criminal may have had access to specific personal information identified below between February and May 20, 2020.

Once Blackbaud detected the intrusion, it was able to halt further system access. As a result, the cyber-criminal only gained access to certain back-up files in specific Blackbaud solutions. Blackbaud, in conjunction with the FBI, investigated the incident and ultimately paid a ransom to the cyber-criminal under the assurance that any exfiltrated files would be destroyed, and their system was fully restored after ransom payment. Through vigilant monitoring post-incident, Blackbaud reports that there has been no evidence of improper use of any of the data files that may have been exposed. Blackbaud has already implemented changes to their data security protocols to prevent a similar incident from occurring again.

What Was Exposed? Wildwood received notice of this incident in July 2020, including information on the specific Blackbaud Solution back-ups exposed. We immediately took action to understand the potential exposure and scope of personal data, and retained counsel to assist and advise. As a result of the ransomware attack, there was exposure of your child's first/last name, phone number, address, date of birth, and medical vaccination record. No other sensitive personal information or financial information was exposed, as all such information is encrypted.

What You Can Do:

We advise you to remain vigilant in reviewing your account statements, monitoring and placing a fraud alert on your child's free credit reports, if they exist. Please refer to the enclosed information for the resources available to you, and the steps that you can take to further protect your child's personal information.

Security experts suggest that you contact your child's financial institution and all major credit bureaus immediately to inform them of such a breach and then take whatever steps are recommended to protect your child's interests, including the possible placement of a fraud alert on your child's credit file, if it exists.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call Kroll at 1-XXX-XXX-XXXX, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time. Kroll representatives have been fully

versed on the incident and can answer questions or concerns you may have regarding protection of your child's personal information.

Because Blackbaud is widely used, other organizations you support may likewise be contacting you. We sincerely apologize for this incident and regret any inconvenience it may have caused you.

Sincerely,
Mark Gutierrez
Director of IT

Additional Important Information

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

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
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

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