



PRINCETON DAY SCHOOL

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

RE: Important Security Notification. Please read this entire letter.

Dear <<Name 1>>:

We are writing to inform you of a data security incident experienced by Blackbaud, Inc. (“Blackbaud”), a provider of cloud-based financial database management services to Princeton Day School, as well as many other not-for-profit organizations, schools, colleges and universities worldwide.

What Happened:

On Thursday, July 16, 2020, we were notified by Blackbaud that it had discovered and stopped a ransomware attack that occurred in May 2020. Blackbaud’s systems that were affected by the attack included a database containing limited historic data related to PDS vendors. According to the notification provided by Blackbaud, the attacker(s) may have acquired an unknown amount of data maintained within Blackbaud’s database. They reported that any account information, usernames, passwords, and Social Security numbers that may have been present in the affected systems were properly encrypted and the decryption keys were not compromised. Blackbaud also informed us that it had paid a ransom to the attacker and obtained confirmation that the compromised information had been destroyed and is no longer in the possession of the attacker(s). According to Blackbaud, and as far as we know, there is no indication that any of the compromised information has been subject to misuse or to further disclosure. Blackbaud has also assured us that they are enhancing their safeguards to mitigate the risk of future attacks. Nevertheless, out of an abundance of caution, we wanted to advise you of this incident and provide you with resources to protect your personal information.

What Information Was Involved:

According to Blackbaud’s initial notification, bank account information, usernames, passwords, and Social Security numbers that may have been entered into the affected systems were encrypted and the decryption keys were not compromised. However, on September 29, 2020, Blackbaud provided an update indicating that certain vendor tax identification numbers that should have been encrypted, were in fact not encrypted by Blackbaud and were therefore potentially exposed. Specifically, Blackbaud indicated that the impacted information was stored in a legacy version of Blackbaud’s financial solution which has not been used by PDS in many years. This legacy data should have been deleted by Blackbaud, and was not encrypted. Notably, Blackbaud indicated that this information was stored in a location only accessible to, and known by, Blackbaud. You are receiving this notification because you were included as a vendor in our Blackbaud database at the time when PDS utilized this legacy solution, and we have confirmed that your information was stored within the unencrypted database. Inclusion as a vendor is not due to full-time employment with PDS, but rather contracted work such as consulting, athletic officiating, providing temporary or one-time services, etc.

We are working diligently to obtain additional information from Blackbaud in order to better understand why this information was not encrypted. Based on our internal investigation, it appears that your social security number was originally provided as a tax identification number and was therefore impacted according to the information provided by Blackbaud.

What Is Being Done:

Blackbaud has indicated that they are taking efforts to further secure their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms. They are deleting the legacy database that was compromised, and have hired a third-party team of experts to monitor the dark web as an extra precautionary measure. Additionally, Blackbaud is offering complimentary credit monitoring services to protect the security of your personal information. Information regarding the credit monitoring services being offered by Blackbaud are provided below.

Credit Monitoring:

You are being provided 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, you are being provided 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 within 90 days from the date of this letter. Information regarding how to enroll in these services is provided on the following pages.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

Should you have questions or concerns regarding this matter, please do not hesitate to contact 855-914-4677. The security of personal information is of the utmost importance to us and we deeply regret this incident. We have made clear to Blackbaud that we expect to receive information regarding the incident, why this information was not properly secured and what steps were taken by Blackbaud to remediate it. Again, according to Blackbaud, and as far as we know, there is no indication that any of the compromised information has been subject to misuse or to further disclosure.

We remain committed to protecting your trust in us and continue to be thankful for your support of Princeton Day School. Please accept our regret for any worry or inconvenience that this incident may cause you.

Sincerely,



Jon Ostendorf
Chief Information Officer



Dulany Gibson
Assistant Head of School for Finance and Operations

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

Credit Monitoring Services

Proactive Fraud Assistance. For sensitive breaches focused on customer retention, reputation management, or escalation handling, 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 includes the following features:

- Fraud specialist-assisted placement of fraud alert, protective registration, or geographical equivalent, in situations where it is 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).
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Answering any questions individuals may have about fraud.
- Provide individuals with the ability to receive electronic education and alerts through email. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

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. ID Theft and Fraud Resolution includes, but is not limited to, the following features:

- Unlimited access during the service period to a personal fraud specialist via a toll-free number.
- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparation of all documents needed for credit grantor notification, and fraud information removal purposes.
- All phone calls needed for credit grantor notification, and fraud information removal purposes.
- Notification to any 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 credit file freezes in states where it is available and in situations where it is warranted (United States only); this is limited to online-based credit freeze assistance.
- Customer service support for individuals when enrolling in monitoring products, if applicable.
- Assistance with review of credit reports for possible fraudulent activity.
- Unlimited access to educational fraud information and threat alerts. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

How do I enroll for the free services?

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

<https://www.cyberscouthq.com/epiq263?ac=XXXXXXX>. If prompted, please provide the following unique code to gain access to services: XXXXXXX

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.** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

➤ PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE

An **initial 1-year security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

TransUnion

Fraud Victim Assistance Dept.
P.O. Box 6790
Fullerton, CA 92834
1-800-680-8289
www.transunion.com

Experian

National Consumer Assistance
P.O. Box 1017
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax

Consumer Fraud Division
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

➤ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. 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. In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail: 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 five (5) years, the addresses where you have lived over the prior five years; 5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); 7. Social Security Card, pay stub, or W2; 8. 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.

➤ ORDER YOUR FREE ANNUAL CREDIT REPORTS

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➤ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

➤ USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements.

Be proactive and create alerts on credit cards and bank accounts to notify you of activity.

If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➤ BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

➤ **RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)**

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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to your employees; (v) you may limit “prescreened” offers of credit an insurance you get based on information in your credit report; (vi) and you may seek damages from a violator. 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

➤ **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

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. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at <http://www.annualcreditreport.com>. Under Rhode Island and Massachusetts law, you have the right to obtain any police report filed in regard to this incident.

- Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.
- **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.
- **For New York residents**, you may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection/>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>
- **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.