Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

June 8, 2021

[redacted]

Dear [redacted]

We are writing to follow up on the letter that we sent to our community on August 31 about a security incident that occurred at one of the School's longstanding vendors, Blackbaud, Inc. As was noted in our letter in late August, Blackbaud is a third-party vendor whose cloud-based software is used by thousands of educational institutions and nonprofit organizations in more than 60 countries for fundraising, records management, and other purposes. St. Mark's has used Blackbaud's software solutions for well over two decades, as it is a widely recognized technology provider among independent schools. Blackbaud recently informed us that it discovered, as part of its on-going investigation, that the security incident may have been more widespread than it initially thought and may have involved additional personal information, including your Social Security number.

As was reported in our August notification, Blackbaud had informed client organizations that use its products, including St. Mark's, that it had discovered and stopped a ransomware attack that targeted Blackbaud's systems. According to Blackbaud, during the incident a file containing personal information was accessed by the threat actor, but Blackbaud paid a ransom to ensure the file was permanently destroyed. In addition, Blackbaud informed us that while the compromised file contained information from some of our data management systems, no Social Security numbers, bank account numbers, or credit or debit card numbers were exposed. As soon as St. Mark's learned of this security incident on Blackbaud's systems, we promptly notified all impacted constituents.

Subsequent to the late August notification that we sent to our community about this incident, Blackbaud informed St. Mark's that information from an additional database, containing data about certain individuals who previously had applied for admission to the School, was also accessed by the threat actor. Blackbaud originally obtained this information when, as part of a software update, it converted data from software previously used by St. Mark's. Blackbaud failed to disclose until now that it had maintained an unencrypted backup file containing information that included the Social Security numbers of individuals whose admission applications had been stored in the software previously used by St. Mark's.

Blackbaud has informed us and other clients that it is continuing to work closely with law enforcement and cyber security experts to monitor the internet to ensure that none of the information that might have been accessed in this incident is misused in any way. Based on the nature of the incident and the research performed by Blackbaud and third-party investigators to date, Blackbaud has reported that there is no reason to believe that any data has been or will be misused, or that it will be disseminated or otherwise made available publicly. Blackbaud has also shared that they have implemented a variety of changes and improvements to strengthen security measures and better protect information from any subsequent incidents, including by addressing the vulnerability that was exploited in this case.

Since learning of this incident, St. Mark's has undertaken extensive measures to address this situation directly, including the following: First and foremost, we have been in constant communication with Blackbaud representatives to ascertain what individuals in our community, if any, might have been directly affected. This has been an arduous process, as we are reliant on disclosures from Blackbaud and want to be certain that we have accurate and complete information. In addition, since learning of this incident, we have been working closely with legal counsel that specializes in cyber-crime and engaged independent technology systems specialists to conduct our own threat assessment and penetration testing of our systems, networks, and protocols on campus, in addition to what is done customarily.

As always, we take the protection and stewardship of the information in our care extremely seriously. We fully recognize that the trust you place in the School is precious and that we must uphold the highest standards at all times to maintain that trust. Please be assured that we will continue to aggressively pursue and monitor this incident and know that we are carefully considering ways to further mitigate potential risks in our community. And, if needed, please know that we will report any and all information of concern to you immediately.

We regret any inconvenience or concern that this incident may cause you, and we will continue to closely monitor the situation. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at cto@smtexas.org.

Thank you for your support of St. Mark's School of Texas.

Sincerely,

Thomas Eckel

Thomas Eckel
Chief Technology Officer

Information About Blackbaud Security Incident

What information was involved?

The information about you in the databases maintained by Blackbaud that may have been accessed includes your Social Security number, contact information, date of birth, and ethnicity.

Credit Monitoring, Proactive Fraud Assistance, and Remediation Support from Blackbaud.

To help protect your identity, Blackbaud is providing you with access to 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, Blackbaud is 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. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter. Further details are contained below.

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 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 security 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.)

ADDITIONAL DETAILS REGARDING YOUR 24-MONTHS OF FREE CREDIT MONITORING SERVICES:

To enroll in Credit Monitoring services at no charge:

- Please navigate to: https://www.cyberscouthq.com/.
- If prompted, please provide the following unique code to gain access to services: **263HQ1765.**
- 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.

We recommend that you continue to review your accounts and free credit reports for suspicious activity, consistent with best practices.

Other important information.

You may contact one of the three major credit bureaus listed below and request that a fraud alert be placed on your credit report or request a copy of your credit report:

Equifax	**Experian**	**TransUnionCorp**
P.O. Box 105873	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013-2002	Chester, PA 19022
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or obtain information about fraud alerts, security freezes, and preventing identity theft:

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