ST. HILDA'S & ST. HUGH'S

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>> <<Date>>
<<Country>>

Dear <<Name 1>>:

St. Hilda's & St. Hugh's School ("SHSH") writes to make you aware of an incident involving one of our third-party vendors, Blackbaud, Inc. ("Blackbaud") that may affect the privacy of some of your information. Blackbaud is a data service provider we use for our development efforts at the school and have previously used for financial reporting and education records. *While we have no evidence of any actual or attempted misuse of any information as a result of this incident*, this notice provides information about the Blackbaud incident, our response and efforts to obtain additional information from Blackbaud, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

**What Happened?** On Thursday, July 16, 2020, SHSH received notification from Blackbaud of a cyber incident on its network. Blackbaud reported that it experienced a ransomware incident in May 2020 that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data from Blackbaud's network at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. In its July 16, 2020 notice, Blackbaud reported that certain information, such as Social Security numbers, financial information, and credit card information, were encrypted within the Blackbaud systems and, therefore, were not accessible to the threat actor. SHSH relied on these assertions to assure certain members of its community on July 18, 2020 that this information had not been impacted by the Blackbaud incident.

Upon receiving notice from Blackbaud, SHSH immediately commenced an investigation to better understand the incident and any impact on SHSH data. This investigation included working diligently to gather further information from Blackbaud. On September 29, 2020, more than two months after first notifying SHSH, Blackbaud notified SHSH again, and stated that, contrary, to its previous representations, certain Social Security numbers, financial information, and vendor information, may have been affected by the Blackbaud incident. Blackbaud reported that at some historical point, this information had been transferred into an unencrypted state without SHSH's knowledge. Following this update, SHSH requested additional information from Blackbaud to confirm the individuals whose sensitive information may have been stored in a Blackbaud system at the time of the incident. On November 9, 2020, Blackbaud provided SHSH access to potentially affected data. SHSH promptly reviewed this information and our records for the purposes of notifying individuals of the Blackbaud incident. On November 9, 2020, Blackbaud provided SHSH access to potentially affected data. SHSH promptly reviewed this information and its records for the purposes of notifying individuals of the Blackbaud incident.

**What Information was Involved?** Based on the information received from Blackbaud, our investigation determined that the involved Blackbaud systems contained your name and Social Security number. Please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by an unknown actor, nor has Blackbaud reported any actual or attempted misuse of SHSH information.

**What We Are 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 reviewing our existing procedures regarding our third-party vendors. SHSH is continuing to work with Blackbaud to address relevant questions and next steps Blackbaud is taking to remediate its data privacy event. Please note that Blackbaud confirmed it will be removing this historical unencrypted SHSH information from its network. We will also be notifying state regulators, as required.

Although SHSH is unaware of any actual or attempted misuse of your information as a result of this incident, we are offering you access to credit monitoring services through CyberScout for twenty-four (24) months at no cost to you as an added precaution. A description of these services and instructions on how to enroll can be found within the enclosed "Steps You Can Take to Help Protect Your Information." Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

**What You Can Do?** We encourage you to remain vigilant against incidents of fraud or identity theft and to monitor your accounts and free credit reports for suspicious activity and to detect errors. Please also review the enclosed "Steps You Can Take to Help Protect Your Information" for general information on what you can do to help protect your personal information.

**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 contact us at **800-823-0005**, Monday through Friday from 9 am to 9 pm EST. You may also write to St. Hilda's & St. Hugh's School at 619 W. 114th Street, New York, NY 10025.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Virginia Connor

Virginia Connor
Head of School

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR MINOR'S INFORMATION

**Enroll in Credit Monitoring**

**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=263HQ1746**

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

**263HQ1746**

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.

**Description of Credit Monitoring Services**

We are 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. 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.

**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.)

**Monitor Accounts**

Under U.S. law you are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, 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. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| P.O. Box 9554 | P.O. Box 160 | P.O. Box 105788 |
| Allen, TX 75013 | Woodlyn, PA 19094 | Atlanta, GA 30348-5788 |
| 1-888-397-3742 | 1-888-909-8872 | 1-800-685-1111 |
| www.experian.com/freeze/center.html | www.transunion.com/credit-freeze | www.equifax.com/personal/credit-report-services |

To request a security freeze, you will need to provide the following information:

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, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one (1) year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

| **Experian** | **TransUnion** | **Equifax** |
|---|---|---|
| P.O. Box 9554 | P.O. Box 2000 | P.O. Box 105069 |
| Allen, TX 75013 | Chester, PA 19106 | Atlanta, GA 30348 |
| 1-888-397-3742 | 1-800-680-7289 | 1-888-766-0008 |
| www.experian.com/fraud/center.html | www.transunion.com/ fraud-alerts | www.equifax.com/personal/credit-report-services |

**Additional Information**

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. 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); or TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

*For New Mexico residents*, 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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. 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 www.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.

*For New York residents*, the Attorney General can be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.