Archbishop Moeller High School

Notice of Data Breach

October 16, 2020

[First Name] [Last Name]
[Address 1]
[Address 2]
[City], [State] [Zip Code]

Dear [First Name]:

Archbishop Moeller High School ("Moeller") utilizes Blackbaud, Inc. ("Blackbaud") for data services that help advance its mission. In connection with those services, Moeller provides your personal information to Blackbaud. I am writing to inform you of a recent data breach experienced by Blackbaud that may have exposed your personal information.

What Happened

Blackbaud was the target of a ransomware attack and data theft that affected certain back-up information related to the Moeller's general ledger. It is believed that the attackers gained unauthorized access to Blackbaud's systems in February of 2020; however, Blackbaud did not notify Moeller of the attack until July 16, 2020, and did not provide complete details of the information affected until September 29, 2020. You can learn more about this incident and Blackbaud's response at https://www.blackbaud.com/securityincident.

What Information Was Involved

Although most personal information stolen during the incident was contained in encrypted fields, Blackbaud notified us on September 29, 2020 that some of your sensitive personal information may have been contained in unencrypted fields, specifically your unencrypted Social Security Number. Blackbaud represented to us that it believes the stolen data was deleted by the attackers. Moeller cannot independently verify whether any of your information was in fact accessed or misused by the attacker.

What We Are Doing

Upon learning of the data breach, we immediately worked with Blackbaud to understand the scope of the data breach, the nature of the information stolen, and the scope of information that was encrypted. We also conducted our own internal investigation into the information affected in the data breach. We are currently working with privacy legal counsel to further investigate the incident, evaluate our relationship with Blackbaud, and ensure Blackbaud takes appropriate measures to protect against similar incidents in the future.

What You Can Do

Please review the attached supplement (*Steps You Can Take to Further Protect Your Information*) for additional steps you can take to protect your information.

In addition, we are providing you with **Single Bureau Credit Monitoring** services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your credit file, a notification is sent to you the same day the change or update takes place with the credit 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. For more information about these services, please review the attached supplement (*Summary of CyberScout Identity Protection Services*). In order for you to receive the monitoring services described above, **you must enroll by March 27, 2021.**

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

- https://www.cyberscouthq.com/epiq263?ac=263HQ1102

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

- 263HQ1102

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 additional step to fully authenticate and activate the services, and receive alerts.**

For More Information

We are working quickly to minimize harm to all affected individuals, and we thank you for your understanding. For further information and assistance, please contact Jeff Gaier at (513) 618-9651 between 8:00AM-4:00PM during the business week or email jgaier@moeller.org.

Sincerely,

Jeff Gaier
Director of Technology
Archbishop Moeller High School

Summary of CyberScout Identity Protection Services

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 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.)

Steps You Can Take to Further Protect Your Information

You can take the following additional steps to protect your information:

- *Review Your Credit Reports and Notify Law Enforcement of Suspicious Activity*

As a precautionary measure, we recommend that you remain vigilant over the next twelve to twenty-four months by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should immediately report it to the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

You have the right to obtain any police report filed concerning this incident. If you are the victim of identity theft, you also have the right to file and obtain a copy of a police report.

To file a complaint with the FTC, go to http://www.identitytheft.gov or call 1-877-ID-THEFT (1-877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- *Obtain A Copy of Your Credit Report*

We recommend that you periodically obtain and review a copy of your credit report from each nationwide credit reporting agency, and have any information relating to fraudulent transactions deleted. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by:

(1) visiting http://www.annualcreditreport.com,
(2) calling toll-free 1-877-322-8228, or
(3) by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the form at: https://www.annualcreditreport.com/manualRequestForm.action.

You can also elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

- *Place A Fraud Alert on Your Credit Report*

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 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 credit reporting agencies identified above.

- *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 may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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. 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, all security freezes are available free of charge. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

Additional information is available via the FTC at https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

- *Additional Free Resources on Identity Theft*

You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information, please visit https://www.identitytheft.gov/Info-Lost-or-Stolen or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft is available on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

- *Additional Resources for New York Residents*

If you are a New York resident and would like to submit inquiries to the New York Attorney General's Office, please contact the Bureau of Internet and Technology (BIT) at:

Bureau of Internet and Technology (BIT)
(212) 416-8433
ifraud@ag.ny.gov
28 Liberty Street
New York, NY 10005
https://ag.ny.gov/bureau/internet-bureau