Archmere ACADEMY

3600 Philadelphia Pike
Claymont, Delaware 19703
(302) 798-6632
archmereacademy.com

October 30, 2020

«Addressee»
«Address_Line_1»
«Address_Line_2»
«City», «State» «Zip»

RE: Updated Notice of Data Breach

Dear «Salutation»,

We write to update you about a security incident of which we previously notified the Archmere community. This letter provides additional information about that incident and explains steps you can take to protect yourself.

What Happened and What Information Was Involved

In July, our third-party service provider, Blackbaud, Inc., notified us that it had experienced a ransomware attack that may have involved access to some of the data we store with Blackbaud. Initially, Blackbaud informed us that the personal information compromised in the security incident did not include Social Security Numbers or bank account numbers. On September 29, 2020, Blackbaud provided us updated information regarding its investigation of the incident. **We now know that your Social Security Number was included in the file that was accessed by the cybercriminal. Also included in the file was a bank account number, ending in «EFT_Last_4», which was associated with your record and likely used for tuition payments.**

It is important to reiterate that based on the nature of the incident, Blackbaud's research, and third party (including law enforcement) investigation, Blackbaud has no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made publicly available. Nonetheless, Blackbaud is offering identity theft services at no cost to you, and we recommend you review the information included with this letter on steps you can take to protect against identity theft. For more information about the security incident and frequently asked questions, please visit our Security Incident Resource Center at https://www.archmereacademy.com/SIRC.

What You Can Do

We are notifying you so that you can take prompt action to protect yourself. We recommend you notify your financial institution that your information may have been compromised by the security incident. **Because the incident may have disclosed your Social Security Number, Blackbaud is offering credit monitoring services at no cost to you.** We recommend you enroll in those services.

Services

Blackbaud is 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, 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 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.** To learn more about what is included in the credit monitoring services, please visit our Security Incident Resource Center at https://www.archmereacademy.com/SIRC.

Enrollment Instructions

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. To enroll in credit monitoring services at no charge, navigate to: https://www.cyberscouthq.com/epiq263?ac=263HQ1104. If prompted, provide the following unique code to gain access to services: [redacted]

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.**

For other steps you can take to protect your information, please see the included "Steps You Can Take to Further Protect Your Information" document, or visit our Security Incident Resource Center at https://www.archmereacademy.com/SIRC. As a best practice, we encourage you to remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities.

For More Information

Archmere Academy takes the protection and proper use of your information very seriously. Archmere is reviewing its procedures and policies for sharing data with our service providers, and taking steps to improve our practices to better protect the personal information entrusted to us by our constituents. We sincerely apologize for this incident and regret any inconvenience it may cause you. For more information about the security incident and frequently asked questions, please visit our Security Incident Resource Center at https://www.archmereacademy.com/SIRC. Should you have any further questions or concerns regarding this matter or the protections available to you, please do not hesitate to contact the Security Incident Response Team at securitynotice@archmereacademy.com or 302-798-6632 ext. 747.

Sincerely,

Michael A. Marinelli, Ed.D. '76

Headmaster

Archmere Academy

Archmere ACADEMY

3600 Philadelphia Pike
Claymont, Delaware 19703
(302) 798-6632
archmereacademy.com

Steps to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should 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 (FTC).

If your personal information has been misused, visit the FTC's site at http://www.identitytheft.gov or call 1-877-ID-Theft (877-438-4338) to file an identity theft complaint and get recovery steps. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database available to law enforcement agencies.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, your state attorney general, or the consumer protection agency in your jurisdiction.

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or 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 request form at https://www.annualcreditreport.com/manualRequestForm.action. Or you can 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 to request a copy of your credit report or for general inquiries is provided below:

Equifax	**Experian**	**TransUnion**
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19016

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

Fraud Alert

You may want to consider placing a fraud alert on your credit report. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor take extra steps to verify your identity, such as contacting you before establishing any accounts in your name. There is no fee to place a fraud alert on your credit report. An initial fraud alert will stay on your credit file for one year unless you choose to remove it sooner. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. They will share your request with the other credit reporting companies. Additional information is available at http://www.annualcreditreport.com.

Security Freeze

You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without your permission. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. That makes it less likely that an identity thief can open new accounts in your name. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place, lift, or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources on Identity Theft

You may wish to review the tips and publications provided by the Federal Trade Commission on how to avoid and recover from identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

You also may wish to visit the website of your state's attorney general or the consumer protection agency of your jurisdiction for further information on steps you can take to prevent identity theft.

District of Columbia residents can obtain information on avoiding identity theft from the Office of the Attorney General at https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft, or by sending an email to oag@dc.gov or calling 202-727-3400.

Maryland residents may wish to review the information provided by the Maryland Attorney General on how to avoid identity theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.statemd.us or calling 410-576-6491.

North Carolina residents can obtain information provided by the North Carolina Attorney General on preventing identity theft by calling 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000, writing to 114 West Edenton Street, Raleigh, NC 27603 or visiting https://ncdoj.gov/protecting-consumers/protecting-your-identity/.