



# THE BOYS' LATIN SCHOOL OF MARYLAND

[Date]

[Name]

[Street Address]

[City, State, Zip Code]

To [Name]:

The Boys' Latin School of Maryland ("The Boys' Latin School") writes to inform you of an incident that may affect the privacy of some of your personal information.

**What Happened?** On Thursday, July 16, 2020, The Boys' Latin School received notification from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including The Boys' Latin School. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on The Boys' Latin School's data. This notice provides information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

Blackbaud reported that in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to investigate. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that data was exfiltrated by the unknown actor at some point before Blackbaud locked the unknown actor out of the environment on May 20, 2020. Upon learning of the Blackbaud incident, The Boys' Latin School immediately began to determine what, if any, sensitive information of ours was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the scope of the incident. On September 29, 2020, The Boys' Latin School of Maryland received supplemental correspondence which advised that certain data was possibly disclosed. After further investigation into this supplemental report, we determined that your information was potentially impacted.

**What Information Was Involved?** Our investigation determined that the involved Blackbaud systems contained your name and Social Security number. Please note that, to date, we have not received any information from Blackbaud that your information was specifically accessed or acquired by the unknown actor.

**What We Are Doing.** We take the confidentiality, privacy, and security of information in our possession very seriously. As part of our ongoing commitment to the privacy of personal information in our care, The Boys' Latin School has taken and is taking steps to review its policies, procedures and existing security measures including the security measures in place at its third-party vendors. Blackbaud has provided you with access to Single Bureau Credit Monitoring services at no charge. Enrollment instructions are located in the enclosed *Steps You Can Take to Help Protect Your Information* document. We will also be notifying state regulators as necessary.

**What You Can Do.** We encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find 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 call our dedicated assistance line at [call center phone number] between the hours of [X and X]. You may also write to The Boys' Latin School of Maryland at 822 W. Lake Ave., Baltimore, MD 21210.

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

Sincerely,

[Signature]

Sean Kriebel  
Assistant Headmaster / CFO

## **STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION**

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.
- And more.

### **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=263HQ1158>**

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

**263HQ1158**

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.

### **Monitor Accounts**

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://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**  
**P.O. Box 9554**  
**Allen, TX 75013**  
**1-888-397-3742**

**[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)**

**TransUnion**  
**P.O. Box 160**  
**Woodlyn, PA 19094**  
**1-888-909-8872**

**[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)**

**Equifax**  
**P.O. Box 105788**  
**Atlanta, GA 30348-5788**  
**1-800-685-1111**

**[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)**

In order 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 (5) 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 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 (7) years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

**Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com/fraud-victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

**Equifax**

P.O. Box 105069 Atlanta,  
GA 30348  
1-888-766-0008  
[www.equifax.com/personal/credit-report-services](http://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](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); 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.

**For Maryland residents**, the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov). **For New York residents**, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>. **For District of Columbia residents**: The District of Columbia Attorney General can be reached at: 441 4th St NW #1100, Washington, DC 20001, [oag.dc.gov](http://oag.dc.gov), (202) 727-3400.