

**NOTICE OF DATA BREACH**

Dear **XXX**

We are writing to let you know that Blackbaud (one of our third party vendors) informed us on July 16, 2020 that they were the victims of a ransomware attack in which files containing information about Athenian and some of our alumni and vendors were accessed and downloaded. At that time, Blackbaud informed us that the information obtained in the attack was encrypted. Based on this representation, our legal counsel determined that Athenian did not need to provide notice to the affected individuals since their information was not at risk of being misused.

On September 29, 2020, Blackbaud provided Athenian an updated notice stating that some of the exposed information was unencrypted. Based on that update we are now providing you the below information to inform you about the original breach, the information that was exposed, and steps we are taking in response.

**What Happened**

According to Blackbaud, cybercriminals gained access to their system as part of a ransomware attack sometime between February 7, 2020 and May 20, 2020. Blackbaud informed us that upon discovering the attack, Blackbaud's cybersecurity team – along with independent forensics experts and law enforcement – stopped the attack and expelled the cybercriminals. However, Blackbaud discovered that prior to locking the cybercriminals out, they removed a copy of a backup file containing your personal information. Blackbaud has assured us, based on representations by the Federal Bureau of Investigations, that upon receiving the ransomware payment the cybercriminals destroyed the information that they accessed.

**What Information Was Involved**

Blackbaud originally represented that your social security number was not exposed. However, in their updated notice, Blackbaud informed us that they believe your social security number was exposed during the incident because they were storing this information in an old version of the Blackbaud software that has since been updated.

**What We Are Doing**

Despite Blackbaud's assurances that the information was destroyed, we are notifying you so that you can take immediate action to protect yourself. Ensuring the safety of your data is of the utmost importance to us. To that end, Blackbaud is offering Identity Theft Protection services to individuals whose social security numbers were exposed at no cost to you. This

service will last for 24 months from the date of enrollment. When changes are made to your Experian credit file, a notification will be sent to you the same day that the change or update takes place with the credit bureau. Additionally, the credit monitoring service comes with the following features:

- ❖ **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 will be 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.)

➤ **Enrollment Instructions**

To enroll in Credit Monitoring services at no charge, please visit: <https://www.cyberscouthq.com/epiq263?ac=263HQ1112>. If prompted, please 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.** In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

In addition to the above steps, Blackbaud intends to encrypt all social security number data in its database by the end of October and delete the old, unused data by the end of this year (2020). Further, Athenian recently instituted a policy of not storing our vendors' social security numbers in Blackbaud's systems.

**What You Can Do**

We recommend you take advantage of the credit monitoring service above and remain vigilant in protecting your identity. Promptly report any suspicious activity or suspected identity theft to the law enforcement.

You should also obtain a copy of your credit report, free of charge, once every twelve months from each of the three nationwide credit reporting agencies. You may also seek to have information relating to fraudulent transactions removed from your credit report. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228.

**For More Information**

Should you have any questions or concerns regarding this matter please do not hesitate to contact me at 925-362-7262 or [ltullo@athenian.org](mailto:ltullo@athenian.org).

If you have questions regarding the credit monitoring service from Cyber Scout please contact them directly at 1-888-682-5911.

### **Additional Resources**

Contact information for the three nationwide reporting agencies is below:

<b>Equifax</b> P.O. Box 740241 Atlanta, GA 30374 866-349-5191 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian</b> P.O. Box 4500 Allen, TX 75013 888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion</b> P.O. Box 160 Woodlyn, PA 19094 833-395-6938 <a href="http://www.transunion.com">www.transunion.com</a>
--	---	--

**Security Freeze.** You can contact the above agencies to place security freezes on your credit report with them for free. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. 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; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

**Fraud Alert.** You may also place a fraud alert in your file by calling one of the three agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

We take this matter very seriously because we know how important your personal information is to you. We know that this situation is concerning to you. Please know we take your support, and your trust, very seriously. We hope our actions moving forward will demonstrate this.

Sincerely,

Louis W. Tullo  
Director of Educational Technology