**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 tax identification number was not exposed. However, in their updated notice, Blackbaud informed us that they believe your tax identification number was exposed 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. Therefore, we will no longer enter or store tax identification numbers in Blackbaud's systems. Instead, Athenian will store tax identification numbers in

Athenian's internal file repositories that contain their own encryptions and are also stored behind a firewall. The tax identification numbers that have not yet been moved and remain in Blackbaud's system are currently encrypted. Blackbaud informs us that it is deleting the versions of it software that stores the unencrypted tax identification numbers by the end of this year (2020).

**What You Can Do**

We recommend that you remain vigilant to the possibility of fraud and corporate identity theft by monitoring your account statements and credit report for any unauthorized activity. Promptly report any suspicious activity or suspected identity theft to law enforcement authorities.

**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.

**Additional Resources**

Contact information for the three nationwide reporting agencies is below:

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| P.O. Box 740241 | P.O. Box 4500 | P.O. Box 160 |
| Atlanta, GA 30374 | Allen, TX 75013 | Woodlyn, PA 19094 |
| 866-349-5191 | 888-397-3742 | 833-395-6938 |
| www.equifax.com | www.experian.com | www.transunion.com |

**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