

October 2020

Dear Friend,

We are writing to let you know that Blackbaud, one of the League of American Orchestras' database vendors, recently notified us of a data security incident that may have involved your personal information. We have been informed by **Blackbaud that this breach did not include access to any credit card information, bank account information, or social security numbers.** Furthermore, based on the nature of the incident, their research, and third party (including law enforcement) investigation, **Blackbaud concluded that there is no reason to believe that any data was or will be misused, or will be disseminated or otherwise made available publicly.**

Notwithstanding Blackbaud's assurances that there is a very low risk that any of your information could be misused, the League of American Orchestras takes the protection and proper use of your information very seriously. We are therefore contacting you to explain the incident and to provide you with additional steps you can take to protect yourself.

### What Happened

Blackbaud, which works with many nonprofits and educational institutions to support their development and donor engagement activities, recently notified us of a security incident. You may have received a similar e-mail about this incident from other nonprofits or universities whose data Blackbaud stewards. At this time, we understand that Blackbaud discovered and stopped a ransomware attack. After discovering the attack, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—expelled the cybercriminal from their system. Blackbaud indicated, however, that the cybercriminal did remove a copy of a backup file containing some of your information before being locked out of the system. A full description of the incident is available on Blackbaud's website at <https://www.blackbaud.com/securityincident>.

### What Information Was Involved

**The cybercriminal did not access your credit card information, bank account information, or social security number.** However, Blackbaud has determined that the file removed may have contained personal information, such as your physical and email addresses, telephone numbers, demographic information, and a history of your relationship with our organization, including donation dates and amounts.

Blackbaud informed us that the company paid the cybercriminal's demand and received confirmation that the copy they removed had been destroyed. As noted above Blackbaud concluded that there is no reason to believe that any data went beyond the cybercriminal, that the data was or will be misused, or that the data will be disseminated or otherwise made available publicly.

## **What Blackbaud and the League are Doing**

The League is notifying you out of an abundance of caution. Ensuring the safety of our constituents' data is of the utmost importance to us.

Blackbaud has assured us of its commitment to prevent future cyber theft, having already implemented several changes to better protect your data.

Blackbaud's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. The company has confirmed through testing by multiple third parties, including the appropriate platform vendors, that its fix withstands all known attack tactics. Additionally, Blackbaud is accelerating their efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

## **What You Can Do**

Although we currently have no reason to believe that your information will be misused, we encourage you to remain vigilant and promptly report any suspicious activity or suspected identity theft to us, to Blackbaud, and to the proper law enforcement authorities.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have any further questions or concerns, please do not hesitate to contact us by email at [securitybreach@americanorchestras.org](mailto:securitybreach@americanorchestras.org) or by phone at 646-822-4098.

Sincerely,



Marc Martin  
Senior Director of Finance and Administration