PRYOR CASHMAN LLP
New York | Los Angeles | Miami
7 Times Square, New York, NY 10036-6569 Tel: 212-421-4100 Fax: 212-326-0806
www.pryorcashman.com

Luke Rushing

Direct Tel: 212-326-0255
Direct Fax: 212-326-0806
LRushing@PRYORCASHMAN.com

October 9, 2020

VIA EMAIL
Donnelle Brooke
Washington State Office of the Attorney General

Re: Data Breach Notification

Dear Ms. Brooke:

Pryor Cashman LLP, represents the American Symphony Orchestra League (the "League"). On behalf of our client, the League, we are reporting a data breach that was perpetrated upon a third-party vendor which the League uses to store donor information. Here is the relevant information:

- **Reporter**
  - Robert J. deBrauwere, Esq.
  - Pryor Cashman LLP
  - rdebrauwere@pryorcashman.com
  - (212) 421-4100
- **Breach Victim**
  - American Symphony Orchestra League, d.b.a. League of American Orchestras
  - 520 8th Avenue, Suite 2005, 20th Floor, New York, NY 10018
  - The League of American Orchestras leads, supports, and champions America's orchestras and the vitality of the music they perform. Founded in 1942 and chartered by Congress in 1962, the League links a national network of thousands of instrumentalists, conductors, managers and administrators, board members, volunteers, and business partners. Its diverse membership of 1,800 organizations and individuals across North America includes world-renowned orchestras, community groups, summer festivals, student and youth ensembles, conservatories, libraries, businesses serving orchestras, and individuals who love symphonic music.
- **Nature of the Breach and Remediation**

- The League uses Blackbaud, a data services vendor, to maintain records of donors to the League. The Blackbaud databases are maintained off-site and are not administered by the League. In August of 2020, the League received a notification from Blackbaud that in May of 2020, Blackbaud was subjected to a ransomware attack. Blackbaud's cybersecurity team, along with independent forensic experts and law enforcement, ultimately expelled the intruders from Blackbaud's system. Prior to expelling the ransomware attackers from its systems, the cybercriminals removed the information in question. To prevent dissemination of any personal data, Blackbaud paid a demand to the cybercriminals, and received confirmation from the cybercriminals that the data had been destroyed. Nonetheless, out of an abundance of caution, the League plans to notify its donors of the breach incident.
- The League has sought and received assurances from Blackbaud that additional measures are being taken to protect the integrity of the League's donor information stored with Blackbaud, including 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.

- **Number of Washington Residents Affected**
  - 1355
- **Information Taken**
  - A subset of potentially personal information for the League's donors, including physical and email addresses, telephone numbers, demographic information, and a history of the donor's relationship with the League, including donation dates and amounts. This exfiltration did not include access to any credit card information, bank account information, or social security numbers.
- **Notification to Affected Individuals**
  - Will be sent *en masse* the week of 10/5/20
  - Template copy of notification attached
  - Will be sent by email to all donors who have a current email address on file, and via US Mail for all donors who have only a postal address
- **Notification to Credit Reporting Agencies**

  - Sent to all three CRAs on 10/2/20

- **Credit Monitoring Services Offered**
  - None at this time.

Please let me know if there are further reporting requirements or any questions I can help with.

Very truly yours,

Luke Rushing
Associate

League of American Orchestras

Advancing the Orchestral Experience for All

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. You can also contact the following credit reporting bureaus and government agencies for more information about how to take steps to avoid identify theft, including placing a fraud alert or implementing a credit freeze.

Credit Reporting Bureaus

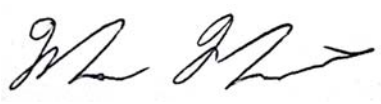
Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

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 or by phone at 646-822-4098.

Sincerely,



Marc Martin
Senior Director of Finance and Administration