



February 16, 2018

Re: Notice of Data Breach

Dear Current and Former LA Phil Colleagues:

I am writing to make you aware of a recent email spoofing attack that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? The Los Angeles Philharmonic was the victim of a targeted email spoofing scheme on February 14, 2018. A request was made from what appeared to be a legitimate LA Philharmonic email address for all 2017 LA Philharmonic employee W-2 information. Unfortunately, copies of all 2017 employee W-2 forms were provided before we discovered that the request was made from a fraudulent account by someone using the name and an email address that appeared to be from our office. We discovered the fraudulent nature of the request on February 14, 2018 and have been working tirelessly to investigate and to mitigate the impact of the attack, and to provide you with helpful resources you can use to avoid any misuse of your personal information.

What Information Was Involved? A file, including a copy of your IRS Tax Form W-2, was sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information. Other than information contained on the IRS Tax Form W-2, no personal financial information was emailed to the external email account.

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. The LA Philharmonic has stringent security measures in place to protect the security of information in our possession. There is no indication the individual who sent the fraudulent email accessed our computer network or that our IT systems were otherwise compromised by this attack. As part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems. We contacted the IRS, state tax authorities and FBI. We will also be contacting the relevant state Attorneys General.

Complimentary Credit Monitoring and Identity Restoration Services

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (myTrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code CODE and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, three-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code 697267 and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the online or offline credit monitoring service anytime between now and June 30, 2018. Due to privacy laws, we cannot register you directly. Please note that credit monitoring and identity restoration services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score. The identity restoration assistance is available to you for two years from the date of this letter with no enrollment required. If you believe you may be a victim of identity theft please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code 697267 to speak to a dedicated TransUnion representative about your identity theft issue.

Beginning Monday, February 19, 2018 at 9:00ET, a dedicated call center will also be available at 855-372-0944 to respond to any additional questions you might have about this incident in particular.

What You Can Do. You can review the enclosed “Steps You Can Take to Prevent Identity Theft and Fraud”. You can also enroll to receive the free credit monitoring and identity restoration services described above.

In addition, if you have not already done so, we encourage you to file your 2017 tax return as soon as possible. If you become aware of a fraudulent tax return filed in your name or you are instructed to do so by the IRS, you should file the IRS Form 14039 Identity Theft Affidavit along with a paper copy of your return and mail according to the instructions on that form. A copy of this form can be found at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>, or <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have questions that are not answered in this letter, please contact TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code 697267 to speak to a dedicated TransUnion representative about your identity theft issue.

The LA Philharmonic takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in black ink that reads "Alison Sowden". The signature is written in a cursive style with a long, sweeping flourish at the end.

Alison Sowden

Vice President, Chief Financial Officer

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts

File Your Tax Return. We encourage you to file your tax return as soon as possible, if you have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You should also look to the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state's tax authority, visit <http://www.taxadmin.org/state-tax-agencies>.

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. 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 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.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently

remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/	freeze.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting 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; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. This notice has not been delayed as the result of a law enforcement investigation.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.