

August 23, 2024

Brian H. Myers
(202) 626-7695 (Direct)
brian.myers@wilsonelser.com

Via Email:

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Cybersecurity Incident

Office of the Attorney General:

Our office represents the Joffrey Ballet (“the Joffrey”), located at 10 E. Randolph St, Chicago, Illinois 60601, and we are providing notice of a recent cybersecurity incident (hereinafter, the “Incident”). By providing this notice, the Joffrey does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

This letter will serve to inform you of the nature of the Incident, what information may have been involved, and the steps that the Joffrey has taken in response to the Incident. We have also enclosed hereto a sample copy of the notice letter we are mailing to the individuals whose personal information was involved starting on August 23, 2024.

1. Nature of the Incident

On September 30, 2023, the Joffrey detected it had experienced a cybersecurity event whereby an unauthorized third party gained access to the Joffrey’s network, encrypted certain files, and left a ransom note. Immediately upon discovering the incident, the Joffrey engaged specialized cybersecurity professionals to secure its network and conduct a forensic investigation. The investigation determined that the unauthorized actor copied certain files from the Joffrey’s network, some of which included personal information. Based upon these findings, the Joffrey reviewed the copied files for the purpose of notifying individuals whose personal information may have been included in those files.

2. Number of individuals and information involved.

The Joffrey’s investigation determined that the personal information of 24 Maryland residents was involved. While the information involved varies for each individual, the Joffrey’s investigation determined that the unauthorized actor may have had access to files containing the

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Los Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

following categories of information: name, date of birth, Social Security number, passport number, driver's license or state identification number, credit or debit card number, financial account number, user ID and password, and health information. Again, the information involved varies for each individual, and not every category applies in each individual case.

As of the date of this letter, the Joffrey is not aware of this incident resulting in any misuse of any personal information for fraud or identity theft.

3. Steps taken in response to the Incident.

Protecting the personal information of its patrons is one of the Joffrey's highest priorities. Upon detecting this incident, the Joffrey immediately retained a leading forensic investigation firm to quickly and thoroughly investigate while securing and safeguarding its network environment. The Joffrey also deployed additional monitoring tools and took additional steps to bolster its security systems. The Joffrey is dedicated to maintaining a best in class data management system that protects its patrons' information and does everything possible to mitigate the risk of any future exposure.

As part of the Joffrey's ongoing commitment to information privacy and security, the individualized notification letters that the Joffrey will mail starting on August 23, 2024 include an offer of complimentary credit monitoring, dark web monitoring, and identity theft restoration services for 12 months, along with instructions on how to enroll in those services.

4. Contact information

If you have any questions or need additional information, please do not hesitate to contact me at Brian.Myers@WilsonElser.com or (202) 626-7695.

Regards,

Wilson Elser Moskowitz Edelman & Dicker LLP



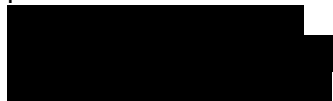
Brian H. Myers, Esq.
Certified Information Privacy Professional, United States (CIPP/US)

Encl.

Joffrey Ballet
c/o Cyberscout, a Transunion Company
PO Box 1286
Dearborn, MI 48120-9998



P



August 23, 2024

Re: Notice of Data Security Incident

Dear [REDACTED]:

The Joffrey Ballet recently completed an investigation into a data security incident that may have exposed your personal information. While we concluded that the incident did not appear to result in any fraud, identity theft or misuse of any personal information, we are writing to share with you the incident details and the steps we are taking to protect your data. Data security is one of our highest priorities and we apologize for any inconvenience.

What Happened:

On September 30, 2023, The Joffrey Ballet detected it had experienced a cybersecurity event whereby an unauthorized third party gained access to the Joffrey's network, encrypted certain files, and left a ransom note. Immediately upon discovering the incident, the Joffrey engaged specialized cybersecurity professionals to secure its network and conduct a forensic investigation. The investigation determined that the unauthorized actor copied certain files from the Joffrey's network, some of which included personal information. Based upon these findings, the Joffrey reviewed the copied files for the purpose of notifying individuals whose personal information may have been included in those files. You are receiving this letter because you may have been one of them.

What Information Was Involved:

Although the Joffrey is not aware of this incident resulting in any misuse of any personal information for fraud or identity theft, we are notifying you for full transparency and out of an abundance of caution. Based on the investigation, the copied files may have included the following categories of your personal information: Financial Account Number.

What We Are Doing:

Protecting the personal information of our patrons is one of our highest priorities. Upon detecting this incident, we immediately retained a leading forensic investigation firm to quickly and thoroughly investigate while securing and safeguarding our network environment. We also deployed additional monitoring tools and took additional steps to bolster our security systems. We are dedicated to maintaining a best in class data management system that protects your information and does everything possible to mitigate the risk of any future exposure.

As part of our ongoing commitment to information privacy and security, we are notifying you of this incident and providing twelve (12) months of **free credit monitoring services**. Upon your completion of the enrollment process you will have access to monitoring of your TransUnion credit file as well as a TransUnion credit report and credit score at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you experience any fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

000010103G0500

P

What You Can Do:

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest you contact your financial institution and all major credit bureaus to inform them of this incident. Please take the appropriate steps recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Additional Information* to learn more about how to protect against the possibility of information misuse.

To enroll in credit monitoring services at no charge, please log on to <https://www.mytrueidentity.com> and follow the instructions provided. When prompted, please provide the following unique code to receive services: [REDACTED]. Please note that the code is case-sensitive and must be entered as it appears.

To receive the monitoring services described above, you must enroll within 90 days from the date of this letter. Enrollment requires an internet connection and e-mail account and may not be available to minors under 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information to confirm your identity for your own protection.

For More Information:

Representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the helpline 1-833-531-2367 and supply the specialist with the unique code listed above. Call center representatives have been fully versed in the incident and can answer questions or concerns regarding protecting your personal information.

While we can assure you that we have not found any evidence that your information was misused for identity theft, we encourage you to take full advantage of the data protection services offered. At The Joffrey Ballet, we are taking every possible step to protect your personal information. And, again, we apologize for any inconvenience.



Shari Massey
Acting President and CEO, Deputy Director and Chief Financial Officer
The Joffrey Ballet

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found on the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.



FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, 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), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.

For Iowa residents, you can report any suspected identity theft to law enforcement or to the Attorney General.

For Massachusetts residents, it is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Maryland residents, if you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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 violators. 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 at 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.

For New York residents, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.

For Oregon residents, state law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For Rhode Island residents, this incident involves 1 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll-free in Vermont only).



