Lynda Jensen
Office: (267) 930-2303
Fax: (267) 930-4771
Email: Ljensen@mullen.law

3 Allied Drive, Suite 303
Dedham, MA 02026

March 12, 2025

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Minnesota Orchestral Association ("MOA") located at 1111 Nicollet Mall, Minneapolis, MN 55403, and are writing to notify your office of an event that may affect the security of certain personal information relating to four (4) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MOA does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On January 21, 2024, MOA detected suspicious activity in its environment. MOA secured its systems and, with the assistance of third-party cybersecurity specialists, investigated to confirm the nature and scope of the activity. The investigation determined that, between January 1, 2024 and January 22, 2024, an unauthorized actor accessed or acquired certain data from MOA systems.

MOA worked with third-party cybersecurity specialists to review the accessible data to identify any sensitive information contained within and the individuals to whom that information relates. MOA then undertook a separate review to locate contact information for those individuals. MOA finalized this review process on February 27, 2025 and worked to notify identified individuals without delay.

The information that could have been subject to unauthorized access includes name, Social Security number and financial account information.

Notice to Maryland Residents

On or about March 12, 2025, MOA provided written notice of this event to four (4) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, MOA moved quickly to investigate and respond to the event, assess the security of MOA systems, and identify potentially affected individuals. Further, MOA notified federal law enforcement regarding the event. MOA is also working to implement additional safeguards and training to its employees. MOA is providing access to credit monitoring services for one (1) year, through TransUnion to individuals whose personal information was accessible during this event, at no cost to these individuals.

Additionally, MOA is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. MOA is providing individuals with information on how to place fraud alerts and credit freezes on their credit files, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

MOA is providing written notice of this event to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2303.

Very truly yours,

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ/ogf
Attachment

EXHIBIT A

Minnesota Orchestral Association
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

MINNESOTA ORCHESTRA

March 11, 2025

Minnesota Orchestral Association ("MOA") is writing to inform you of an event that involves your personal information. This notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened. On January 21, 2024, MOA detected suspicious activity in our environment. We secured our systems and, with the assistance of third-party cybersecurity specialists, investigated to confirm the nature and scope of the activity. The investigation determined that, between January 1, 2024 and January 22, 2024, an unauthorized actor accessed or acquired certain data from MOA systems.

MOA worked with third-party cybersecurity specialists to review the accessible data to identify any sensitive information contained within and the individuals to whom that information relates. We then undertook a separate review to locate contact information for those individuals. MOA finalized this review process on February 7, 2025 and worked to notify identified individuals without delay.

What Information Was Involved. The following types of personal information related to you were present in the accessible data at the time of the event: name, .

What We Are Doing. MOA takes this event and the security of information in our care seriously. Upon detecting the activity, we secured our network, initiated an investigation, and reviewed potentially affected data in order to notify individuals. We also notified federal law enforcement and will be notifying applicable regulators. As part of our ongoing commitment to the privacy and the security of our environment, we are also reviewing our existing policies and procedures.

MOA is providing you with **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services 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. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. MOA is also providing you with guidance on how to help protect your personal information, should you feel it is appropriate to do so. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself.

What You Can Do. MOA encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and by monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information in the enclosed *Steps You Can Take to Help Protect Personal Information*. There, you will find additional information about the complimentary credit monitoring services and how to enroll.

For More Information. We understand you may have questions about this event that are not addressed in this letter. If so, please call our dedicated assistance line at: 1-855-577-9042. This toll-free line is available Monday through Friday 8:00 AM - 8:00 PM EST (excluding major U.S. holidays).

Sincerely,

Minnesota Orchestral Association

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial, as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-442-9828; and https://oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6400; and www.ncdoj.gov.