



Jason Cherry, Esq.
2029 Century Park East
Suite 1100
Los Angeles, CA 90067
jcherry@constangy.com
Tel.: 207.745.1397

April 1, 2024

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notification of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith, and Prophete LLP represents Detroit Symphony Orchestra (“DSO”) in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in compliance with Maine’s data breach notification statute.

1. Nature of the Security Incident

On September 27, 2023, the DSO became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, the DSO immediately took steps to secure its digital environment. The DSO also engaged leading cybersecurity experts to assist with an investigation and to determine whether personal information may have been accessed or acquired without authorization. The investigation revealed that an unknown actor gained access to and obtained certain data from the DSO network between September 19 to September 27, 2023. The DSO then worked with additional experts to conduct a comprehensive review of the impacted data to determine what personal information was involved. On or about March 26, 2024, DSO determined that personal information was impacted in connection with this incident.

2. Number of Affected Maine Residents Notified

On April 1, 2024, the DSO notified 4 Maine residents by letter mailed via first class U.S. mail. A sample copy of the notification letter is included with this correspondence.

The impacted information varies by individual but may include the residents’ name along with their social security number, driver’s license number or state identification number, financial account number, and routing number.

3. Measures Taken to Address the Incident

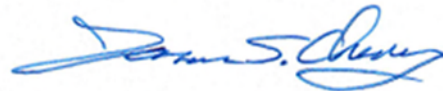
In response to the incident, the DSO retained cybersecurity experts and launched a forensics investigation to determine the source and scope thereof. The DSO implemented additional security measures to further harden its environment in an effort to prevent a similar event from occurring in the future. The DSO also reported this incident to federal law enforcement and will cooperate with any investigation.

The DSO is notifying the affected individuals and providing resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity protection services to each individual whose personal information was affected by this event, including 12 months of credit monitoring, identity restoration services, and identity protection insurance. Those services are offered through Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. Cyberscout will also support a call center for at least 90 days to answer questions and assist with enrollment.

4. Contact Information

The DSO takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at 207.745.1397 or jcherry@constangy.com.

Sincerely yours,



Jason S. Cherry of
CONSTANGY, BROOKS, SMITH &
PROPHETE LLP

Encl.: Sample Consumer Notification Letter

Detroit Symphony Orchestra
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



April 1, 2024

Subject: Notice of Data Security Incident

Dear [REDACTED]:

The Detroit Symphony Orchestra (DSO) is writing to inform you of a recent data security incident that involved your personal information. At the DSO, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On September 27, 2023, the DSO became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, we immediately took steps to secure our digital environment. We also engaged leading cybersecurity experts to assist with an investigation and to determine whether personal information may have been accessed or acquired without authorization. The investigation revealed that an unknown actor gained access to and obtained certain data from the DSO network between September 19 to September 27, 2023. The DSO then worked with additional experts to conduct a comprehensive review of the impacted data to determine what personal information was involved. On or about March 26, 2024, we determined that your personal information was impacted in connection with this incident.

What Information Was Involved? The information involved included your name along with your [REDACTED].

What We Are Doing? As soon as we discovered this incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future.

DSO is also notifying you of this incident and offering you the opportunity to enroll in complimentary credit monitoring and identity theft protection services by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. These services include 12 months credit monitoring, identity restoration services, and identity protection insurance.

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/dso> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. Please note the deadline to enroll is June 30, 2024.

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.

000010102G0400

P

What You Can Do. We encourage you to enroll in the complimentary identity protection services we are offering. With this protection, Cyberscout can help you resolve issues if your identity is compromised. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information: Cyberscout 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 am to 8:00 pm Eastern Time, Monday through Friday, excluding holidays. Please call the help line at 1-833-919-9503 and supply the specialist with your unique code listed above.

We thank you for your understanding deeply regret any worry or inconvenience that this may cause.

Very truly yours,

A handwritten signature in black ink, appearing to read "Linda Lutz", with a stylized flourish at the end.

Linda Lutz
Vice President & Chief Financial and Administrative Officer
Detroit Symphony Orchestra
3711 Woodward Ave.
Detroit, Michigan 48201

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com
--	---	---

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Internal Revenue Service Identity Protection PIN (IP PIN): You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here:
<https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.



Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and
Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

**North Carolina Attorney
General**

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

**Rhode Island Attorney
General**

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

**Washington D.C. Attorney
General**

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit:
<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>