



Matthew Toldero, Partner
Cybersecurity & Data Privacy Team
One West 4th Street, Suite 850
Winston-Salem, NC 27101
mtoldero@constangy.com
Mobile: 336.448.8552

August 19, 2025

VIA ONLINE SUBMISSION

Attorney General Mike Hughes
Office of the Attorney General
Consumer Protection Division
2115 State Capital
Lincoln, NE 68509
Email: ago.consumer@nebraska.gov

Re: Houston Symphony Society - Notice of Data Event

Dear Attorney General Hughes:

We represent Houston Symphony Society (“Houston Symphony”), located at 615 Louisiana Street, Suite 102, Houston, Texas 77002, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately five (5), Nebraska residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Houston Symphony does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

1. Nature of the Data Event

On July 2, 2025, Houston Symphony learned that personal information of certain individuals was potentially accessed without authorization. The unauthorized access was the result of a suspicious event Houston Symphony first learned of on or about February 5, 2025. Specifically, Houston Symphony identified access to its network systems. Upon learning of this activity, Houston Symphony immediately took steps to secure its network systems and engaged digital forensics specialists to assist with an investigation.

On February 27, 2025, the investigation revealed that certain files were accessed or acquired without authorization. Houston Symphony then undertook a comprehensive review of the files to determine what potentially affected data was involved and whether they included any sensitive data. When this process was completed on or about July 2, 2025, it was first determined that personal information belonging to certain individuals was affected. Houston Symphony then worked diligently to effectuate notification to potentially affected individuals. Please note, Houston Symphony has no evidence of the misuse or attempted misuse of any potentially accessed information.

The information that could have been subject to unauthorized access includes first and last name, as well as Social Security number.

2. Notice to Nebraska Residents

On or about August 19, 2025, Houston Symphony provided written notice of this incident to approximately five (5), Nebraska residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

3. Other Steps Taken and To Be Taken

Upon discovering the event, Houston Symphony moved quickly to investigate and respond to the incident, assess the security of Houston Symphony's network systems, and identify potentially affected individuals. Houston Symphony also implemented additional safeguards and training. Houston Symphony is providing access to credit monitoring services for 24 months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals, and is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Houston Symphony is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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.

4. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (336) 448-8552.

Very truly yours,

A handwritten signature in cursive script that reads "Matt Toldero".

Matt Toldero of
Constangy, Brooks, Smith & Prophete LLP



Houston Symphony Society
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS1550

HOUSTON
SYMPHONY



August 19, 2025

Subject: Notice of Data Security Breach

Dear 

We are writing to inform you of the data security incident recently experienced by Houston Symphony Society (“Houston Symphony”) that may have affected your personal information. We take the privacy and security of all information within our possession seriously. Please read this letter carefully as it contains information regarding the incident, the actions we took in response and steps that you can take to help protect your personal information.

What Happened. The Houston Symphony detected unauthorized network access as the result of suspicious activity on February 5, 2025, at which time we immediately took steps to protect our systems, initiate an investigation and engage cybersecurity experts to assist our team. We also notified law enforcement.

On February 27, 2025, the investigation revealed that certain files were accessed or acquired without authorization. We then undertook a comprehensive review of the files to determine what potentially affected data was involved and whether they included any sensitive data. When this process was completed on or about July 2, 2025, we determined that personal information belonging to you may have been affected. Since that time, we’ve worked diligently to identify current contact information in order to notify all individuals whose personal information may have been affected. Please note that Houston Symphony has no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information may have included your name and driver or state license number; financial account number with access info; and, Social Security number. Although additional data elements unrelated to you were impacted, the investigation found no evidence that the ticket sales and donors’ database (encrypted and stored by a third-party network) was involved, though certain older financial accounts data stored elsewhere may have been affected.

What We Are Doing. As noted above, upon learning of the suspicious activity we took steps to protect our systems and enhance security measures, initiated an investigation and engaged cybersecurity experts to assist our team. Our response to this event also included notifying federal law enforcement. We have been working diligently to investigate this matter as well as to provide

you with notice of the incident. Safeguarding your information is a top priority, and we continually assess our security measures to ensure that best practices are in place to secure our systems and minimize the risk of a similar incident occurring in the future.

We have no evidence of the misuse or attempted misuse of any potentially impacted information as a result of this incident; however, out of an abundance of caution, Houston Symphony is offering you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24 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 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.

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: [REDACTED] In order for you to receive the monitoring services described above, you must enroll within 120 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.

What You Can Do. We urge you to act proactively to avoid identity theft, including by reviewing the recommendations in the enclosed “Steps You Can Take to Help Protect Your Personal Information.” We also encourage you to enroll in the monitoring services being offered to you at no cost through TransUnion by using the enrollment information provided. Please note that we are unable to enroll you in these services; you must enroll directly with TransUnion.

For More Information. We have established a special call center to provide assistance and address any questions you may have. Please call 1-800-405-6108 Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern time, excluding holidays. We take this matter very seriously and appreciate your continued trust in us. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Houston Symphony



Steps You Can Take To Help Protect Your 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 (the "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 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 2000
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 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.

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
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
[www.marylandattorneygeneral.gov/
Pages/CPD](http://www.marylandattorneygeneral.gov/Pages/CPD)
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
[www.doj.state.or.us/
consumer-protection](http://www.doj.state.or.us/consumer-protection)
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General

1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology

28 Liberty Street
New York, NY 10005
[www.dos.ny.gov/consumerprotection/
212.416.8433](http://www.dos.ny.gov/consumerprotection/)

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General

700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General

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

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.