LEWIS BRISBOIS BISGAARD & SMITH LLP

Brian Craig
2112 Pennsylvania Avenue NW, Suite 500
Washington, DC 20037
Brian.Craig@lewisbrisbois.com
Direct: 202.926.2904

December 16, 2020

File No. 34181.584

VIA ELECTRONIC MAIL
Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent Playhouse Square Foundation ("Playhouse Square"), which operates a performing arts center, a hotel and a real estate business in Cleveland, Ohio, in connection with a data security incident described in greater detail below. Playhouse Square takes the protection of all sensitive information within its possession very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. Nature of the security incident.

On June 29, 2020, Playhouse Square became aware of unusual activity within its network environment and discovered that it had been the victim of data encryption by an unknown individual. Upon discovering this activity, Playhouse Square took immediate and active steps to secure its environment and launched an internal investigation with the assistance of a leading independent computer forensics firm. The investigation determined that certain Playhouse Square data may have been accessed or downloaded between June 22 and 29, 2020.

As a result, Playhouse Square promptly undertook a review of the affected data in order to identify any individuals whose personal information was within the potentially affected data. That review concluded on December 7, 2020. Since that time, we have been working diligently to identify up-to-date address information for all potentially affected individuals. On December 11, 2020, we identified one (1) New Hampshire resident within the population.

The potentially affected information pertaining to the New Hampshire resident includes name and payment card information.

2. Number of New Hampshire residents affected.

Playhouse Square is preparing to issue a notification letter to the one (1) New Hampshire resident regarding this data security incident via first-class U.S. mail on December 16, 2020. A sample copy of the notification letter is included with this correspondence.

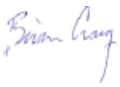
3. Steps taken relating to the incident.

Playhouse Square has taken steps in response to this incident to minimize the likelihood of similar incidents occurring in the future. Those steps include deploying an advanced endpoint detection and response tool on its systems that is monitored by an external cybersecurity firm, and implementing additional employee training. In addition, out of an abundance of caution, Playhouse Square is offering the potentially affected individuals credit monitoring, identity protection services, and identity theft insurance at no cost through IDX.

4. Contact information.

Playhouse Square remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (202) 926-2904 or via email at Brian Craig@lewisbrisbois.com.

Very truly yours,



Brian Craig of
LEWIS BRISBOIS BISGAARD & SMITH LLP

BC:ALW

Attachment: Consumer Notification Letter Template

C/O IDX
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-754-1359
Or Visit:
https://response.idx.us/psf-protect
Enrollment Code: [XXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 16, 2020

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident that may have involved your personal information. At Playhouse Square Foundation ("Playhouse Square"), we take the privacy and security of personal information very seriously. That is why I am notifying you of the incident, offering you complimentary credit monitoring and identity protection services, and informing you about steps you can take to help protect your personal information.

What Happened? On June 29, 2020, Playhouse Square became aware of unusual activity within its network environment and discovered that it had been the victim of data encryption by an unknown individual. Upon discovering this activity, we took immediate and active steps to secure our environment and launched an internal investigation with the assistance of a leading independent computer forensics firm. The investigation determined that certain Playhouse Square data may have been accessed or downloaded between June 22 and 29, 2020, as a result of this incident, and we immediately launched a thorough review of the potentially affected data. Our review concluded on December 7, 2020, and identified that some of your personal information was contained with the potentially affected data. Since that time, we have worked diligently to gather up-to-date contact information for all individuals whose data may have been affected.

Playhouse Square is committed to maintaining the security of all information within our possession. That is why we are contacting you, to offer you credit monitoring and identity protection services for 12 months at no cost.

What Information Was Involved? The potentially affected information may include <<VARIABLE>>.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We have also taken measures to further increase the security of our network environment, including deploying an advanced endpoint detection and response tool on our systems that is monitored by an external cybersecurity firm and implementing additional employee training, to minimize the probability of a similar event occurring in the future.

As an added precaution, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do: You can follow the recommendations included with this letter to protect your personal information. We strongly encourage that you enroll in the complimentary credit monitoring and identity protection services we are offering through IDX to further protect your personal information. To enroll, please visit https://response.idx.us/psf-protect or call 1-833-754-1359 and use the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll in these services is March 16, 2021. To activate credit monitoring you must be over the age of 18, and have established credit in the U.S., a Social Security number in your name, and a U.S. residential address associated with your credit file.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions, please contact our team at 1-833-754-1359 Monday through Friday from 9 am - 9 pm Eastern Time. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Gina M. Vernaci
President and CEO
Playhouse Square Foundation

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review 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 should also 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 http://www.annualcreditreport.com/, calling toll-free 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 can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.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 90 days. 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. 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. There is no charge to place, lift or remove the security freeze. 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. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov or www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
Bureau of Internet and Technology Resources	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
28 Liberty Street	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
New York, NY 10005	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
ifraud@ag.ny.gov	1-888-743-0023	1-877-566-7226	401-274-4400
1-212-416-8433			

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

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft. Contact information for the three national credit reporting agencies may be found below.