BRIAN MIDDLEBROOK
BMIDDLEBROOK@GRSM.COM

GORDON&REES
SCULLY MANSUKHANI
YOUR 50 STATE PARTNER™

ATTORNEYS AT LAW
1 BATTERY PARK PLAZA, 28TH FLOOR
NEW YORK, NY 10004
WWW.GRSM.COM

January 4, 2021

VIA ELECTRONIC MAIL (SECURITYBREACH@ATG.WA.GOV)
Attorney General Bob Ferguson
800 5th Avenue, Suite 2000
Seattle, Washington 98104-3188

Re: Supplemental Notification of Data Security Incident
Our File No: 1220111

Dear Attorney General MacDonald:

As you are aware, this firm represents the interests of The 5th Avenue Theatre Association (the "Theatre") in connection with the above referenced matter. Please allow this to serve as a supplemental notification of data security incident following the notification provided to your office dated September 28, 2020 (the "Notification").

As indicated in the Notification, the Theatre suffered a break in and theft which it first learned of on August 30, 2020. The theft included certain computer black-up tapes and equipment which stored data that appears to have included personal information, including name(s), date(s) of birth, and Social Security number(s). The Theatre has worked actively with law enforcement, a specialized legal team, as well as leading security experts, to determine what specific information may have been stored on and accessible from the stolen equipment and the potential, if any, for unauthorized access to it. This involved a comprehensive manual review and identification process which concluded on December 2, 2020.

While the Theatre believes that the stolen data is extremely difficult to open and requires a high degree of technical expertise to access, the Theatre has provided notification of the incident to potentially impacted individuals in an abundance of caution and so that they are clearly informed of the situation. Following completion of the aforementioned comprehensive manual review and identification process, the Theatre has provided notification to additional potentially impacted individuals *via* written and substitute notice on December 24, 2020, including one thousand one hundred forty-two (1,142) Washington residents. A sample copy of the notification to the Washington residents is attached. The Theatre has also provided notification of the incident to major statewide media and has posted a copy of the notice on the homepage of its website, accessible at: https://www.5thavenue.org/legal/follow-up-theft-of-staff-data/. As noted in the attachment, the Theatre has included in the notification an offer to provide twelve months of one-bureau credit monitoring services to the affected Washington residents.

As stated above, the Theatre has worked actively with law enforcement, a specialized legal team, and leading security experts to investigate the nature of the information stored on and accessible from the stolen equipment and the degree of risk of unauthorized access to it. This incident has been reported to law enforcement and is actively being investigated. At all relevant times, the Theatre maintained and continues to maintain a written information security program for the physical and electronic safeguarding of all information. The Theatre is continuing to work internally and with leading security experts concerning physical and electronic data security to undertake appropriate precautionary measures to ensure that this does not happen again.

Should you have any questions or require additional information, please do not hesitate to contact me.

Best regards,

GORDON REES SCULLY MANSUKHANI, LLP

/s/ Brian Middlebrook

Brian Middlebrook, Esq.

Enclosures

<<Date (Format: Month Day, Year)>>

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

5th Avenue Theatre (the "Theatre") understands the importance of protecting your information and is writing to inform you that the Theatre suffered a break in and theft which it first learned of on August 30, 2020 (the "Incident").

The theft included certain computer back-up tapes and specialized equipment which stored data that appears to have included personal information of some employees, guests and contractors. The Theatre has worked actively with law enforcement, a specialized legal team, as well as leading security experts, to determine exactly what specific information may have been stored on and accessible from the stolen equipment and the potential, if any, for unauthorized access to it, and is providing you with this notice of the Incident in an abundance of caution. This notice describes the Incident, outlines the measures that the Theatre has taken in response, and advises you on steps you can take to further protect your information.

What Happened? The Incident occurred overnight on August 29, 2020 where unauthorized individuals broke into the Theatre, among other offices in the building, and stole certain computer equipment, among other property. Immediately following the Incident, the Theatre contacted law enforcement and retained a specialized legal team and security experts to determine exactly what specific information may have been stored on and accessible from the stolen equipment and the potential, if any, for unauthorized access to it, which involved a comprehensive manual review and identification process of the contents known to be contained on the stolen equipment.

What Information Was Involved? As indicated above, the Theatre has worked actively with law enforcement, a specialized legal team, and leading security experts to determine exactly what specific information may have been stored on and accessible from the stolen equipment. This involved a comprehensive manual review and identification process which identified certain files on the stolen equipment which may have included your name, date of birth and/or Social Security number. This comprehensive review and identification process concluded on or about December 2, 2020. While we believe that the stolen data is extremely difficult to open and requires a high degree of technical expertise to access, the Theatre is providing notice of this Incident to you in an abundance of caution so that you are clearly informed of this situation.

What We Are Doing: As stated above, the Theatre has worked actively with law enforcement, a specialized legal team, and leading security experts to investigate the nature of the information stored on and accessible from the stolen equipment and the degree of risk of unauthorized access to it.

Also, we have secured the services of Kroll to make available identity monitoring services at no cost to you for a period of one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include credit monitoring, fraud consultation and identity theft restoration.

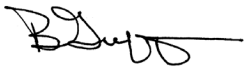
Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.
*You have until **March 17, 2021** to activate your identity monitoring services.*
Membership Number: **<Member ID>>**

Additional information describing your services is included with this letter.

What You Can Do: We know and understand how important your personal information is to you. To protect yourself from potential harm associated with the Incident, we encourage you to enroll in the complimentary identity monitoring service noted above, to closely monitor all mail or other contact from individuals not known to you personally, and to avoid answering questions or providing additional information to such unknown individuals. We also remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements, explanation of benefit statements, and credit reports for unauthorized activity, and to report any such activity or any suspicious contact whatsoever to law enforcement if warranted.

For More Information: For further information on steps you can take to prevent against possible fraud or identity theft, please see the attachments to this letter. The Theatre understands the importance of protecting your personal information, and deeply regrets any concern this may have caused to you. **Should you have any questions and would like further information regarding the information contained in this letter, please do not hesitate to contact 1-866-461-1558**, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. Please have your membership number ready.

Sincerely,



Bernadine C. Griffin
Managing Director, The 5th Avenue Theatre

Attachment 1 – Protecting Yourself

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements and credit reports for unauthorized activity. Residents of the United States are entitled to one free credit report annually from each of the three major credit reporting agencies. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228. 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.

You may want to consider placing a fraud alert on your credit report. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert.

- Initial Alert: You may ask that an initial alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. A fraud alert does not impact your ability to get a loan or credit, but rather alerts a business that your personal information may have been compromised and requires the business to verify your identity before issuing you credit. Although this may cause some delay if you are applying for credit, it may protect against someone else obtaining credit in your name. An initial fraud alert stays on your credit report for at least one year.
- Extended Alert: You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies. The agency that you contacted must notify the other two agencies.

Additionally, you have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. However, unlike a fraud alert, you must separately place a security freeze on your credit file at each of the three national credit reporting agencies. In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Below are the toll-free numbers and addresses for the three largest credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 74021	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Below is the toll-free number, address and website address for the Federal Trade Commission, which you may contact to obtain further information on how to protect yourself from identity theft and how to repair identity theft: Federal Trade Commission; Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/idtheft

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon and West Virginia: It is required by state law to inform you that 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 using the contact information listed above.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023; www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence, RI 02903
1-401-274-4400; www.riag.ri.gov

Office of the Illinois Attorney General
Identity Theft Hotline
100 W Randolph St, Fl. 12
Chicago, IL 60601
1-866-999-5630; www.illinoisattorneygeneral.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226; www.ncdoj.com

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Connecticut, Massachusetts, Rhode Island and West Virginia: You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above.

For residents of Texas: We believe that this incident may have affected 16 Texas residents.

*FAIR CREDIT REPORTING ACT***.** You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Note - Identity theft victims and active duty military personnel have additional rights.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.