BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

November 22, 2016

VIA E-MAIL: SECURITYBREACH@ATG.WA.GOV

Attorney General Bob Ferguson
Washington Office of the Attorney General
1125 Washington St., N.E.
P.O. Box 40100
Olympia, WA 98504

Re: Incident Notification

Dear Attorney General Ferguson:

Our client, The Madison Square Garden Company (MSG), understands the importance of protecting the payment card information of its customers. MSG was notified that payment card issuing banks identified a transaction pattern indicating a potential data security concern. MSG immediately commenced an investigation and engaged leading computer security firms to examine its network. In the last week of October 2016, as soon as the investigation found signs of external unauthorized access, MSG worked with computer security firms to stop it and to implement enhanced security measures. Findings from the investigation show unauthorized access to MSG's payment processing system and the installation of a program that looked for payment card data as that data was being routed through the system for authorization.

Data contained in the magnetic stripe on the back of payment cards swiped in person to purchase merchandise and food and beverage items at Madison Square Garden, the Theater at Madison Square Garden, Radio City Music Hall, Beacon Theater, and Chicago Theater between November 9, 2015 and October 24, 2016 may have been affected, including credit card numbers, cardholder names, expiration dates and internal verification codes. Not all cards used during this time frame were affected. This incident did not involve cards used on MSG websites, at the venues' Box Offices, or on Ticketmaster.

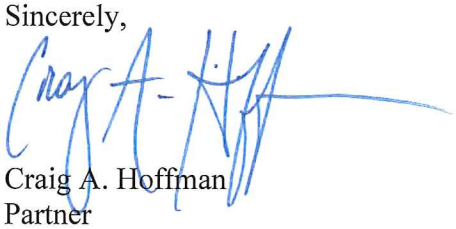
MSG has stopped the incident and taken significant steps to strengthen the security of its network environment. Initial measures taken to contain the attack included resetting all enterprise passwords, blocking certain network communication attempts, implementing two-

factor authentication, and removing and cleaning devices affected by the attack. MSG has also notified law enforcement about the incident. The payment card networks will be working with the banks that issued payment cards used during the affected time period. MSG has also established a dedicated call center that potentially affected individuals can call with questions regarding the incident.

MSG does not collect the mailing or email address from customers when they use their payment card to buy merchandise, food or beverage items. Thus, MSG is not able to identify the name and mailing address of individuals who used their card during the time period of this incident. MSG, therefore, is also unable to identify the number of Washington residents that used a card during the time period of this incident. Instead, pursuant to *Wash. Rev. Code Ann. §19.255.010*, MSG is providing substitute notification today to Washington residents who may have used their payment cards at Madison Square Garden, The Theater at Madison Square Garden, Radio City Music Hall, Beacon Theater, and Chicago Theater during the time period of this incident by posting a statement on its website and issuing a press release (copies enclosed). Notification is being provided in the most expedient time possible and without unreasonable delay following the completion of an investigation by MSG to determine the scope of the incident. *See Wash. Rev. Code Ann. §19.255.010.*

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Craig A. Hoffman
Partner

Enclosure

The Madison Square Garden Company Notifies Customers of Payment Card Incident

New York, NY (November 22, 2016) - The Madison Square Garden Company (NYSE: MSG) is notifying customers that it identified and has addressed a payment card issue. This issue may have affected cards used at merchandise and food and beverage locations at Madison Square Garden, The Theater at Madison Square Garden, Radio City Music Hall, Beacon Theatre and The Chicago Theatre. After MSG was notified that payment card issuing banks identified a transaction pattern indicating a potential data security concern, MSG immediately commenced an investigation and engaged leading computer security firms to examine its network. In the last week of October 2016, as soon as the investigation found signs of external unauthorized access, MSG worked with security firms to stop it and to implement enhanced security measures. MSG is also working with law enforcement regarding this matter.

Findings from the investigation show external unauthorized access to MSG's payment processing system for the properties listed above and the installation of a program that looked for payment card data as that data was being routed through the system for authorization. Data contained in the magnetic stripe on the back of payment cards swiped in person at the MSG locations listed above between November 9, 2015 and October 24, 2016 may be affected, including credit card numbers, cardholder names, expiration dates and internal verification codes. Not all cards used during this timeframe were affected, and this incident did not involve cards used at MSG websites, the venues' Box Offices or on Ticketmaster.

It is important to note that MSG has fixed the issue, and customers may use their cards with confidence at MSG venues.

MSG is providing information on its website, www.themadisonsquaregardencompany.com/customerupdate, regarding steps customers can take to guard against misuse of payment card information. Potentially affected customers are advised to remain vigilant by regularly reviewing their payment card statements for any unauthorized activity. Customers should immediately report any unauthorized charges to their card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of the payment card.

MSG recognizes the importance of protecting customer data and deeply regrets any inconvenience this incident may have caused its customers. MSG has set up a dedicated call center for customer inquiries regarding this matter. Individuals can call 844-319-9619 from 9 a.m. to 9 p.m. EST, Monday to Friday (except major holidays).

Contact: Kimberly Kerns, Kimberly.Kerns@msg.com

The Madison Square Garden Company Notifies Customers of Payment Card Incident
November 22, 2016

California residents please click here

The Madison Square Garden Company ("MSG") understands the importance of protecting payment card data. After MSG was notified that payment card issuing banks identified a transaction pattern indicating a potential data security concern, MSG immediately commenced an investigation and engaged leading computer security firms to examine its network. In the last week of October 2016, as soon as the investigation found signs of external unauthorized access, MSG worked with the security firms to stop it and to implement enhanced security measures.

Findings from the investigation show external unauthorized access to MSG's payment processing system and the installation of a program that looked for payment card data as that data was being routed through the system for authorization. Data contained in the magnetic stripe on the back of payment cards swiped in person to purchase merchandise and food and beverage items at Madison Square Garden, the Theater at Madison Square Garden, Radio City Music Hall, Beacon Theater, and Chicago Theater between November 9, 2015 and October 24, 2016 may have been affected, including credit card numbers, cardholder names, expiration dates and internal verification codes. Not all cards used during this time frame were affected. This incident did not involve cards used on MSG websites, at the venues' Box Offices, or on Ticketmaster.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take to protect your information.

MSG has stopped this incident, and we continue to work with the computer security firms to further strengthen the security of our systems to help prevent this from happening again. We have also been providing information to law enforcement regarding this matter.

MSG values the relationship we have with our customers and understands the importance of protecting personal information. We regret any inconvenience this may have caused. If you have questions, please call 844-319-9619 from 9 a.m. to 9 p.m. EST, Monday to Friday (excluding major holidays).

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com,1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: 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. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. 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.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, 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 credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

If you are a resident of Maryland, North Carolina, or Rhode Island, you may contact and obtain information from your state attorney general at:

- *Maryland Attorney General's Office,* 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland)
- (410) 576-6300 (for calls originating outside Maryland)
- *North Carolina Attorney General's Office,* 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400
- *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400

If you are a resident of Massachusetts, note that pursuant to Massachusetts law, you have the right to file and obtain a copy of any police report.

Massachusetts law also allows consumers to request a security freeze. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

The fee for placing a security freeze on a credit report is $5.00. If you are a victim of identity theft and submit a valid investigative report or complaint with a law enforcement agency, the fee will be waived. In all other instances, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. If you have not been a victim of identity theft, you will need to include payment to the credit reporting agency to place, lift, or remove a security freeze by check, money order, or credit card.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

In order to request a security freeze, you will 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.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.