ANAHEIM
MAJESTIC
GARDEN HOTEL
PREMIER HOTEL COLLECTION

RETURN MAIL PROCESSING CENTER
PO BOX 6336
PORTLAND, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear Valued Customer:

We are writing to you because of an incident involving unauthorized access to customer information associated with your room reservation(s) at the Anaheim Majestic Garden Hotel. The privacy and protection of our customers' information is a matter we take very seriously, and we recommend that you closely review the information provided in this letter for some steps that you may take to protect yourself against potential misuse of your information.

What Happened?

The Anaheim Majestic Garden Hotel had engaged the Sabre Hospitality Solutions SynXis Central Reservations System ("SHS Reservation System") to facilitate online booking of hotel reservations. You may be aware that the SHS Reservation System is a leading online reservations systems used throughout the world.

Last month we received notice from Sabre that an unauthorized party had gained access to payment card information, as well as certain reservation information for a subset of hotel reservations processed through the SHS Reservation System. The unauthorized access included some room reservations at the Anaheim Majestic Garden Hotel which had been processed through the same Reservation System. We are informed that Sabre's investigation determined that the unauthorized party first obtained access to payment card and other reservation information on August 10, 2016, and that the last access to payment card information occurred on March 9, 2017. As per conversation with Sabre, Sabre has removed the compromised account that was used by the unauthorized party.

What Information Was Involved?

We were informed by Sabre that the unauthorized party was able to access payment card information for your room reservation(s) at the Anaheim Majestic Garden Hotel, including the relevant cardholder name, payment card number, payment card expiration date, and, possibly, the applicable payment card security code. Apparently, the unauthorized party was also able, in some cases, to access certain information such as guest name, email address, phone number, street address, and other information. Information such as social security numbers, passport numbers, and driver's license numbers was not accessed.

What We Are Doing

Sabre has informed us that it has engaged a leading cybersecurity firm to support its investigation into this matter, and that it also notified law enforcement and the relevant payment card brands about this incident.

What You Can Do

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your payment card and bank account statements, and by monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, such as your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
https://www.identitytheft.gov/

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the credit reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting agencies to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please 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 credit reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide credit reporting agencies at:

Equifax
P.O. Box 105788
Atlanta, GA 30348
(800) 525-6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(800) 680-7289
www.transunion.com

For More Information

We appreciate your patronage of the Anaheim Majestic Garden Hotel. If you have any questions regarding this incident or if you desire further information or assistance, please do not hesitate to contact your dedicated call center at (844) 327-2358, Monday through Friday, 7am to 7pm Pacific time excluding holidays. To view notice information and certain state-specific information online, please visit www.SabreConsumerNotice.com.

Sincerely yours,

Anaheim Majestic Garden Hotel