GT GreenbergTraurig

Lori S. Nugent
Tel 214.665.3600
Fax 214-665-3601
nugentl@gtlaw.com

July 31, 2017

FIRST-CLASS MAIL
VIA E-MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol St.
Concord, NH 03301
doj-cpb@doj.nh.gov

Re: Voluntary Security Incident Notice Provided for Paris Las Vegas Operating Company, LLC d/b/a Paris Las Vegas

Dear Attorney General Gordon MacDonald,

This firm represents Paris Las Vegas Operating Company, LLC d/b/a Paris Las Vegas ("Paris Las Vegas") with respect to an incident involving the potential exposure of certain personal information on a reservation system owned and operated by Sabre Hospitality Solutions ("Sabre").

Nature of the Incident.
Sabre's SynXis Central Reservations (SynXis) system allows travel agents and others to search for and reserve rooms at thousands of hotels, including at Paris Las Vegas. Paris Las Vegas recently learned that the Sabre SynXis system experienced a data security incident. According to Sabre's investigation, some hotel reservations processed through the SynXis system from August 10, 2016 to March 9, 2017 may have been accessed without authorization. An unauthorized party obtained access to credentials on Sabre's system, which could have permitted unauthorized access to reservation information on Sabre's system, including guests' names and credit card numbers, and also may have included card expiration dates, security codes, and mailing addresses.

The property management systems for Paris Las Vegas were not involved. In addition, Paris Las Vegas never receives credit card information from Sabre for reservation transactions. Instead, Paris Las Vegas processes reservations from Sabre using tokens. As a result, Paris Las Vegas does not receive the guest card holder name, card number, expiration date, or security code that may have been given to Sabre by the guest or the guest's travel agent.

On June 6, 2017, Sabre gave Paris Las Vegas limited information to assist in identifying potentially affected guests. Based on this limited information, Paris Las Vegas was able to

identify some guests whose reservation information may have been involved in Sabre's data security incident.

Because Paris Las Vegas values its guests' privacy and security, Paris Las Vegas is voluntarily notifying affected guests concerning Sabre's data security incident. Paris Las Vegas also is providing its guests with two free years of credit monitoring and identity protection services through Equifax.® We have attached a sample of the notification letters that are being provided to identified guests.

Number of New Hampshire Residents Affected.
The data set at issue included two (2) New Hampshire residents. A notification letter is being sent to these residents via regular mail on July 31, 2017.

Steps Taken and Plans Relating to the Incident.
Paris Las Vegas is providing notification to its guests out of an abundance of caution and encouraging its guests to closely monitor their credit card statements and report any unusual activity. Paris Las Vegas also engaged Epiq Solutions to provide mailing and call centering services, as well as two years of credit monitoring and identity protection services through Equifax® at no cost to the guests.

Contact Information.
Should you have any questions or if additional information is needed, please do not hesitate to contact me at nugentl@gtlaw.com or 214-665-3630.

Best regards,

Lori S. Nugent

Lori S. Nugent
Shareholder

Enclosure

July 31, 2017

«First_Name» «Last_Name»
«Street_Address»
«Address_2»
«City», «State» «Zip»

Dear «First_Name» «Last_Name»

We recently learned that a reservation system owned and operated by Sabre Hospitality Solutions (Sabre) experienced a data security incident. Our systems at Paris Las Vegas were not involved, but Sabre has informed us that information on its system about your reservation at Paris Las Vegas may have been accessed without authorization.

We value the privacy and security of our guests' information, and we are sorry for any inconvenience that Sabre's incident may cause.

What Happened?

Sabre's SynXis Central Reservations (SynXis) system allows travel agents and others to search for and reserve rooms on behalf of their clients at thousands of hotels, including at our property. According to Sabre's investigation, some hotel reservations processed through the SynXis system from August 10, 2016 to March 9, 2017 may have been accessed without authorization. An unauthorized party obtained access to credentials on Sabre's system, which could have permitted unauthorized access to your reservation information.

What Information Was Involved?

Sabre's investigation indicated that certain reservation information may have been accessed without authorization. The information included guests' names and credit card numbers, and also may have included card expiration dates, security codes, and mailing addresses.

On June 6, 2017, Sabre gave us limited information to assist us in identifying guests who may have been affected by this incident. Based on this limited information, we were able to determine that your reservation information may have been involved in Sabre's data security incident. Sabre did not, however, provide us the card holder name or address for the credit card used for the reservation, so we are unable to determine if the credit card used for your reservation belongs to you or another person.

Our hotel never receives credit card information from Sabre for any reservation transactions. To process credit card transactions for reservations made using the Sabre system, credit card information is transmitted from the Sabre system to our third party credit card payment processor.

What Sabre is Doing

Sabre retained a leading cybersecurity firm to investigate the incident. Additionally, Sabre notified law enforcement and the credit card companies about this incident so that they can coordinate monitoring of the credit cards at issue. Sabre has also indicated that it has secured its system.

What We are Doing

Because we value you as our guest, we want to make sure you are aware of this incident. To ease any concern you may have, at no cost to you, we are providing you with two years of credit monitoring and identity protection services through Equifax® as described below.

What Can Affected Individuals Do?

We are alerting you to this incident so that you can take steps to protect your information. It is a good practice to carefully review your credit card statements and quickly report anything unusual to your financial institution or credit card company. There are rules that limit a credit card company's reimbursement for fraudulent credit card charges when a problem is not reported quickly.

As a precautionary measure to help better protect your credit file from potential misuse, we have partnered with Equifax ® to provide its Credit Watch ™ Silver credit monitoring and identity theft protection product for two years at no charge to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code).

If you choose to take advantage of this product, it will provide you with a notification of key changes to your Equifax credit file, up to $25,000 Identity Theft Insurance [1] Coverage, automatic fraud alerts,[2] access to your Equifax credit report and Identity Restoration. If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity.

Even if you decide not to take advantage of the subscription offer, you may still receive Equifax Identity Restoration in the event that you become victim of identity theft by calling 877-368-4940, 9:00 a.m. to 8:00 p.m. Eastern, Monday through Friday, before August 1, 2019.

You must complete the enrollment process for Equifax Credit Watch™ Silver by November 1, 2017. We urge you to consider enrolling in this product, at our expense, and reviewing the attached materials enclosed with this letter.

For More Information

If you have any questions regarding this incident or if you desire further information or assistance, please do not hesitate to contact us at 1-800-572-9349. We are available Monday through Friday from 9:00 a.m. to 9:00 p.m. EST.

Sincerely,

Paris Las Vegas Operating Company, LLC d/b/a Paris Las Vegas
3655 Las Vegas Boulevard, South
Las Vegas, NV 89019

EQUIFAX®

Activation Code: «Redeption_Code»

About the Equifax Credit Watch™ Silver identity theft protection product

Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your Equifax credit file. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- Comprehensive credit file monitoring of your Equifax credit report with daily notification of key changes to your credit file.
- Wireless alerts and customizable alerts available
- One copy of your Equifax Credit Report™
- $25,000 in identity theft insurance with $0 deductible, at no additional cost to you †
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalize identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality *
- Identity Restoration If you become a victim of identity theft, an Equifax identity restoration specialist will work on your behalf to help you restore your identity.

How to Enroll: You can sign up online

To sign up online for **online delivery** go to www.myservices.equifax.com/silver

1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.
2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.
4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

State Notification Requirements

All States.
You may obtain a copy of your credit report or request information on how to place a fraud alert or security freeze by contacting any of the national credit bureaus below. It is recommended 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.

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
1-800-680-7289
Chester, PA 19016
www.transunion.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 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 at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze and free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia.
It is required by state laws 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.

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

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

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

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

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 Unit
(401) 274-4400
http://www.riag.ri.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