McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonaldhopkins.com

July 6, 2017

VIA EMAIL: *SecurityBreach@atg.wa.gov*

Office of Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Four Seasons Hotels Limited ("Four Seasons"). I write to provide notification concerning an incident at Sabre Hospitality Solutions ("Sabre"), a third-party hotel reservations provider to Four Seasons and other hotel companies and travel partners worldwide. This incident may affect the security of personal information of six hundred thirty six (636) Washington residents who are Four Seasons customers. Sabre's investigation is ongoing and this notification will be supplemented with any new significant facts or findings provided to Four Seasons by Sabre subsequent to this submission, if any. By providing this notice, Four Seasons does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

The incident involves unauthorized access to reservation information, including payment card information, made through the Sabre Hospitality Solutions SynXis Centre Reservations System (CRS). Sabre advised Four Seasons that it engaged a leading cybersecurity firm to support its investigation. Sabre also notified law enforcement and major credit card brands about this incident so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used.

Following an examination of forensic evidence, Sabre confirmed to Four Seasons on June 6, 2017 that an unauthorized party gained access to account credentials that permitted unauthorized access to certain unencrypted payment card information, as well as certain reservation information, for a subset of hotel reservations processed through the Sabre CRS. Sabre has confirmed that the issue has been contained and the unauthorized access has been revoked. Sabre's investigation did not uncover evidence that the unauthorized party removed any information from the system, but it is a possibility.

Sabre's investigation determined that the unauthorized party first obtained access to payment card and other reservation information on August 10, 2016. The last access to payment card information was on March 9, 2017.

Reservations made on Fourseasons.com, with Four Seasons Worldwide Reservations Office, or made directly with any of Four Seasons 105 hotels or resorts were not compromised by this incident. Sabre's CRS platform serves thousands of hotel properties in all market segments from independent properties to large global chains; many of these companies and other travel partners have been impacted by this incident.

The unauthorized party was able to access payment card information for *certain* hotel reservation(s), including cardholder name; payment card number; card expiration date; and, potentially, card security code. The unauthorized party was also able, in some cases, to access certain information such as guest name, email, phone number, address, and other information. Information such as Social Security, passport, or driver's license number was not accessed.

To date, Four Seasons has not received any reports of identity fraud, theft or specific misuse of information as a direct result of this incident. Nevertheless, we wanted to make you (and the potentially affected residents) aware of the incident and explain the steps that have been taken to date. The Washington residents impacted by this Sabre incident will be provided with written, electronic and/or substitute notice commencing on July 6, 2017, in substantially the same form as the notice attached hereto, which includes an explanatory letter from Sabre. The residents may contact the Sabre toll-free response line with questions regarding the incident. A microsite has also been made available to the residents.

The residents will also be advised to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis, and to report suspicious activity to their financial institutions. The residents have also been provided with best practices to protect their personal information, including steps to obtain a free credit report, place a security freeze and/or fraud alert on their credit files. The residents also will be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or *dpaluzzi@mcdonaldhopkins.com*.

Sincerely,

Dominic A. Paluzzi

DAP/sdg
Encl.

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Re: Notice of Sabre Data Security Incident

Dear <<Name>>:

We are writing to notify you of a data security incident at Sabre, a third-party hotel reservations provider to Four Seasons Hotels and Resorts and other hotel companies and travel partners worldwide. The incident involves unauthorized access to reservation information, including payment card information, made through the Sabre Hospitality Solutions SynXis Centre Reservations System (CRS). Sabre has confirmed that the issue has been contained and the unauthorized access has been revoked, but some of your information may have been compromised as a result of the incident.

The enclosed letter from Sabre provides additional explanatory information regarding this incident.

What Happened?

The Sabre CRS facilitates the booking of hotel reservations made by consumers through hotels, online travel agencies, and similar booking services. Following an examination of forensic evidence, Sabre confirmed to Four Seasons Hotels and Resorts on June 6, 2017 that an unauthorized party gained access to account credentials that permitted unauthorized access to certain unencrypted payment card information, as well as certain reservation information, for a subset of hotel reservations processed through Sabre's system.

Sabre's investigation determined that the unauthorized party first obtained access to payment card and other reservation information on August 10, 2016. The last access to payment card information was on March 9, 2017. Sabre's investigation did not uncover evidence that the unauthorized party removed any information from the system, but it is a possibility.

It is important to note that reservations made on Fourseasons.com, with Four Seasons Worldwide Reservations Office, or made directly with any of Four Seasons 105 hotels or resorts were not compromised by this incident.

What Information was Involved?

The unauthorized party was able to access payment card information for certain hotel reservation(s), including cardholder name; payment card number; card expiration date; and, potentially, card security code. The unauthorized party was also able, in some cases, to access certain information such as guest name, email, phone number, address, and other information. Information such as Social Security, passport, or driver's license number was not accessed.

What Sabre is Doing

Sabre has engaged a leading cybersecurity firm to support its investigation. Sabre also notified law enforcement and major credit card brands about this incident so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used.

What You Can Do

Enclosed you will find precautionary measures you can take to protect your personal information. You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and 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.

For More Information

Sabre's CRS platform serves thousands of hotel properties in all market segments from independent properties to large global chains; many of these companies and other travel partners have been impacted by this incident. As a result, you may receive multiple notifications about this incident from multiple hotel properties or hotel brands, credit card companies, or other travel partners.

We apologize for any inconvenience that this incident has caused.

If you have any further questions regarding this incident, please call the dedicated toll-free response line at 800-442-8960 (U.S. and Canada) and 503-520-4461 (international). This response line is staffed with professionals familiar with Sabre's data security incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available 24 hours a day, Monday through Friday, with voicemail available outside of those hours. Translation services are available at the response line.

For additional information, you may also visit **http://sabreconsumernotice.com**

– OTHER IMPORTANT INFORMATION –

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and 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 under the federal Fair Credit Reporting Act (FCRA) to request that the credit reporting agency delete that information from your credit report file.

In addition, under the FCRA, 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

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Dear Four Seasons Customers:

Sabre is a leading technology provider to the global travel industry, and counts Four Seasons as one of our most important customers of our Sabre Hospitality Solutions (SHS) division.

SHS had a cybersecurity incident that affects you. We wanted to offer an explanation.

SHS provides reservations technology to a number of hotel companies. SHS had an incident in which an unauthorized party was able to obtain the credentials to an account within the SHS central reservations system and then view a subset of the hotel reservations. This was ***not*** an internal technology platform at a hotel that you stayed at, and the unauthorized use was contained to one system managed by SHS. As part of this incident, payment card information that may have been transmitted as part of the reservation booking process may have been viewed by this unauthorized user.

Sabre engaged premier cybersecurity experts to support our investigation and took successful measures to ensure this unauthorized access was stopped and is no longer possible. The investigation did not uncover evidence that the unauthorized party removed any information from the system, but it is a possibility. We have also notified law enforcement and the payment card brands.

The unauthorized party was able to access information for certain hotel reservations, including cardholder name; payment card number; card expiration date; and, for a subset of reservations, card security code (if it was provided). Social Security, passport, driver's license or other government identification numbers were ***not*** accessed.

On behalf of the Sabre team, we wish to express our sincere regret for this incident and assure you that we have taken measures to further strengthen our already-robust cybersecurity program. As a leading technology provider to the travel industry, Sabre is committed to a global, holistic security program focused on protecting its systems, their customers and consumers. As cyber threats have escalated, so too has Sabre's investment in state of the art security technology and highly qualified personnel to reassure its travel industry customers and the traveling public that Sabre addresses security with the utmost care and expertise.

Yours truly,
SABRE HOSPITALITY SOLUTIONS