NOTICE OF SABRE DATA SECURITY INCIDENT

IMPACTING GUEST PAYMENT CARD INFORMATION

Four Seasons Hotels and Resorts was recently informed of a data security incident at Sabre, a third-party hotel reservations provider to thousands of hotel properties, including those managed by Four Seasons. The incident involved unauthorized access to certain guest information associated with a subset of hotel reservations processed through Sabre's SynXis Central Reservations System (CRS) from August 10, 2016 until March 9, 2017. Sabre has confirmed that the issue has been contained and the unauthorized access has been revoked, but some guest information may have been compromised as a result of the incident.

The below 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.

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, affected individuals may receive multiple notifications about this incident from multiple hotel properties or hotel brands, credit card companies, or other travel partners.

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 Affected Individuals Can Do

Affected individuals should remain vigilant for incidents of fraud and identity theft by regularly reviewing account statements and monitoring free credit reports for any unauthorized activity. If there is any suspicious or unusual activity on accounts, affected individuals should report it immediately to their financial institutions, as major credit card companies have rules that restrict them from requiring payment for fraudulent charges that are timely reported. Below are precautionary measures affected individuals can take to protect their personal information.

For More Information

Four Seasons is working closely with Sabre to ensure Four Seasons guests are notified in a timely manner and provided with appropriate information. Guests with available email or mailing addresses have been sent notification of this incident commencing on July 6, 2017.

For further questions regarding this incident or to determine whether your reservation has been impacted, 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 affected individuals can do to protect against misuse of their 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 visit **http://sabreconsumernotice.com**

– OTHER IMPORTANT INFORMATION –

Affected individuals should remain vigilant for incidents of fraud and identity theft by regularly reviewing account statements and monitoring free credit reports for any unauthorized activity. If there is any suspicious or unusual activity on accounts, affected individuals should report it immediately to their financial institutions, as major credit card companies have rules that restrict them from requiring payment for fraudulent charges that are timely reported.

INFORMATION FOR U.S. RESIDENTS

In addition, affected individuals may contact the Federal Trade Commission (FTC) or law enforcement, such as their state attorney general, to report incidents of identity theft or to learn about steps to take to protect against identity theft. The FTC can be contacted at:

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

If affected individuals find that their information has been misused, the FTC encourages filing a complaint with the FTC and to take these additional steps: (1) close the accounts that are confirmed or believed to 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 a Credit Report

Affected individuals should also monitor their credit reports. U.S. consumers may periodically obtain credit reports from each nationwide credit reporting agency. If inaccurate information or a fraudulent transaction is found on a credit report, individuals have the right under the federal Fair Credit Reporting Act (FCRA) to request that the credit reporting agency delete that information from the credit report file.

In addition, under the FCRA, U.S. consumers are entitled to one free copy of their credit report every 12 months from each of the three nationwide credit reporting agencies. To obtain a free copy of a credit report, go to www.AnnualCreditReport.com or by calling (877) 322-8228. Affected individuals may also 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. Affected individuals may also contact any of the three major credit reporting agencies to request a copy of their credit report.

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

In addition, affected individuals 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	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	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.

Massachusetts Residents: Under Massachusetts law, affected individuals have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion by regular, certified, or overnight mail at the addresses above.

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, 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, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express, or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies 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 identities 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.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity;
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
4. Payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

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

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, (401) 274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

Unless you are sixty-five (65) years of age or older, or you are a victim of identity theft with an incident report or complaint from a law enforcement agency, a consumer reporting agency has the right to charge you up to ten dollars ($10.00) to place a freeze on your credit report; up to ten dollars ($10.00) to temporarily lift a freeze on your credit report, depending on the circumstances; and up to ten dollars ($10.00) to remove a freeze from your credit report. If you are sixty-five (65) years of age or older or are a victim of identity theft with a valid incident report or complaint, you may not be charged a fee by a consumer reporting agency for placing, temporarily lifting, or removing a freeze.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

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. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment. Do not send cash through the mail.

INFORMATION FOR CANADIAN RESIDENTS

Please note that under the *Privacy Act* you are entitled to register a complaint with the Office of the Privacy Commissioner of Canada with regard to this incident. Complaints may be forwarded to the following:

Office of the Privacy Commissioner of Canada
30 Victoria Street
Gatineau (Quebec)
K1A 1H3
Email: notification@priv.gc.ca

Additional information is available on the Privacy Commissioner's website at http://priv.gc.ca.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide credit reporting agency. You may request a free credit report from each of the major credit reporting companies by contacting them at:

- Equifax Canada: 1-800-465-7166; www.equifax.ca
- TransUnion Canada: 1-800-663-9980; www.transunion.ca

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Place a Fraud Alert on Your Credit Report File

You are permitted to place an initial "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts in your name, increase the credit limit on an existing account, or provide a new card on an existing account. To place a fraud alert, contact either of the credit bureaus at the numbers or websites listed above. As soon as one credit bureau confirms your fraud alert, they will notify the other.

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