Cooley

Kris Kleiner
+1 720 566 4048
kkleiner@cooley.com

Via Email to: SecurityBreach@atg.wa.gov

March 2, 2018

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Legal Notice of Information Security Incident

Dear Sir or Madam:

I write on behalf of my client, Preferred Hotels & Resorts ("Preferred"), to inform you of a potential security incident involving the personal information of certain properties within Preferred's portfolio of independent hotels, which may have affected approximately 2,1687 Washington residents. Preferred is notifying these individuals and outlining some steps they may take to help protect themselves.

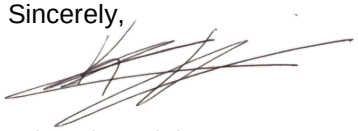
Preferred was recently notified of a potential security incident by Sabre/SynXis, a company that operates an Internet-accessible reservation platform for the hotel industry. According to the information we have received from this vendor, an unauthorized individual was able to gain access to user credentials that enabled the party to view certain reservation information between June of 2016 and November of 2017. Based on the information we have received from the vendor, the information in these reservations that was accessed may have included certain payment card data belonging to certain individuals who provided card details when making reservations at some Preferred hotels. Please note that no Preferred computer or network systems were affected in any way by this incident and Preferred is unaware of any fraudulent activity that has occurred as a result of this incident.

Preferred takes the privacy of personal information seriously, and was deeply disappointed to learn that this incident involving the vendor's systems could affect Preferred guests. Upon learning of the incident, Preferred promptly initiated an investigation into the incident and has communicated extensively with the vendor to learn more about what occurred. The vendor has informed us that it has enhanced the security around its access credentials and the monitoring of system activity to further detect and prevent unauthorized access. In addition, the vendor has advised us that they notified law enforcement and the payment card brands of this incident. Furthermore, Preferred is continuing to take actions, in cooperation with Sabre, to improve the security and protection of all reservations information and to enhance all systems to help prevent this type of incident from recurring.

Affected individuals are being notified starting on or around March 5, 2018. A form copy of the notice being sent to the potentially affected Washington residents is included for your reference. If you have any questions or need further information regarding this incident, please contact me at (720) 566-4048 or kkleiner@cooley.com.

Cooley

Sincerely,



Kristopher Kleiner

Enclosure

[DATE]

[CUSTOMER NAME AND ADDRESS]

Notice of Data Breach

Dear [NAME]:

Preferred Hotels & Resorts ("Preferred"), was recently notified by its service provider, Sabre Hospitality Solutions ("Sabre"), of a data security incident Sabre experienced that may affect certain customer information associated with your hotel reservation(s). The privacy and protection of our customers' information is a matter we take very seriously, and we are providing this notice as a precaution to let you know about the incident and tell you about some steps that you may take to protect yourself against any potential misuse of your information.

What Happened

The Sabre SynXis Central Reservations System (CRS) facilitates the booking of hotel reservations made by consumers through hotels, online travel agencies, and similar booking services. Following their internal investigation, Sabre notified us that an unauthorized party gained access to user credentials that enabled the party to view some reservation information for a subset of hotel reservations that Sabre processed on behalf of some of its customers, including certain Preferred hotel properties. The investigation determined that the unauthorized party was able to access Sabre's system between June of 2016 and November of 2017. Please note that no Preferred computer or network systems were affected in any way by this incident.

What Information Was Involved

Based on the information provided to us by Sabre, it appears that the unauthorized party was able to access payment card information for certain hotel reservations, including cardholder names, card numbers, card expiration dates, and, potentially, card verification codes. The unauthorized party was also able, in some cases, to access certain information such as guest names, emails, phone numbers, addresses, and other information. Because sensitive information such as Social Security, passport, or driver's license numbers are not collected during the hotel reservation process, none of this type of sensitive personal information was affected by this incident.

What We Are Doing

We take the privacy of personal information seriously and deeply regret that this incident occurred. We took steps to address and contain this incident promptly after we were informed, including initiating an internal investigation into the incident and communicating with Sabre to learn more about what occurred. Sabre has informed us that they have taken steps to enhance the security around access credentials and the monitoring of system activity to help prevent this type of incident from recurring in the future. In addition, Sabre has notified law enforcement and the payment card brands about this incident.

What You Can Do

We recommend that you review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not recognize, you should immediately

notify the issuer of the credit or debit card as well as the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

Although Social security numbers and other sensitive personal information were not at risk in this incident, as a general practice you can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. As an additional precaution, we are providing an "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact us directly at [NUMBER] between [TIMES] Central time, Monday through Friday. Again, we sincerely regret any concern this event may cause you.

Sincerely,

[SIGNATURE]

Ken Mastrandrea,

Chief Operating Officer

INFORMATION ABOUT IDENTITY THEFT PROTECTION

Review of Accounts and Credit Reports: As a precaution you may regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the end of this guide.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft. There may be similar resources available at the state level, and you may contact your state department of revenue directly for more information.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: 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.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may request an initial fraud alert 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 request an extended fraud alert 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 at the addresses or toll-free numbers listed below.

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.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.(By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. 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 will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. 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.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

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

Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374
877-478-7625

Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

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

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 1000
Chester, PA 19016
800-888-4213

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872