Preferred Hotel Group, Inc.
d.b.a. Preferred Hotels & Resorts
311 South Wacker Drive
Chicago, IL 60606

**WASHINGTON**

June 30, 2017

VIA E-MAIL TO SECURITYBREACH@ATG.WA.GOV
AND FIRST CLASS MAIL

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

*Re: Incident Notification*

Dear Attorney General Ferguson:

We are writing to notify you of an incident involving the unauthorized access of personal information involving approximately 2,370 Washington residents.

Sabre Hospitality Solutions, a company that facilitates the booking of reservations for Preferred Hotel Group and Historic Hotels of America, either through our member hotels, our call centers, travel agencies, online travel agencies or similar booking services, informed us that an unauthorized party gained access to their SynXis Central Reservations system. We have been told that this unauthorized party could view unencrypted payment card information (as well as certain reservation information) in electronic form, for a subset of hotel reservations processed through their system.

Following an investigation and examination of its forensic evidence, Sabre notified us on June 6, 2017 of the incident. Sabre's investigation determined that the unauthorized party first obtained access to unencrypted payment card and other reservation information for a subset of hotel reservations processed through their system on August 10, 2016. According to Sabre, the last access to payment card or reservation information was on March 9, 2017.

At this time, we are unaware of any fraudulent activity that has occurred as a result of the breach.

Enclosed please find copies of the notices that will be sent to affected individuals by July 6, 2017. If we can provide you with any further information, please do not hesitate to contact me directly via phone at (949) 999-9434 or email at KMastrandrea@preferredhotels.com.

Sincerely,

Ken Mastrandrea
Chief Operating Officer

Cc: Ieuan Jolly, Loeb & Loeb, LLP
ijolly@loeb.com

**[INCLUDE PREFERRED SHORT NOTIFICATION LETTER]**
**[INCLUDE HISTORIC SHORT NOTIFICATION LETTER]**

<<Mail ID>>
<<First_Name>><<Mid_Name>><<Last_Name>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

<<DATE>>

**NOTICE OF DATA BREACH**

Dear <<First_Name>><<Last_Name>>:

We are writing to you because of an incident that we were recently made aware of by one of our service providers, involving the unauthorized access to your personal information associated with your hotel reservation(s).

We take the privacy and protection of your information 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 the potential misuse of your information.

**What Happened?**

Sabre Hospitality Solutions, a company that facilitates the booking of our reservations either through our member hotels, our call centers, travel agencies, online travel agencies, or similar booking services informed us that an unauthorized party gained access to their SynXis Central Reservations system. We have been told that this unauthorized party could view unencrypted payment card information, as well as certain reservation information, for a subset of hotel reservations processed through their system.

Following an investigation and examination of its forensic evidence, Sabre notified us on or about June 6, 2017 of the incident. Sabre's investigation determined that the unauthorized party first obtained access to certain unencrypted payment card and other reservation information for a subset of hotel reservations processed through their system on August 10, 2016. According to Sabre, the last access to payment card or reservation information was on March 9, 2017.

**What Information Was Involved?**

Based on the information Sabre provided to us, we have reason to believe that the unauthorized party was able to access payment card information for your hotel reservation(s), including cardholder name; card number; card expiration date; and, potentially, your card security code. We have been informed that the unauthorized party was also able, in some cases, to access certain information such as guest name, email, phone number, address, and other information if it was included with your reservation. We have been assured that information such as Social Security, passport, or driver's license numbers were not accessed.

**What We Are Doing**

We are currently working with Sabre to ensure they evaluate and improve their data security processes and we are notifying affected guests and our member hotels of this unfortunate incident. Law enforcement, payment card brands and the major credit reporting agencies have also been notified.

**What You Can Do**

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 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 (typically, between $5.00 and $10.00, depending on your state). Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

You may contact the nationwide credit reporting agencies at:

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

**For More Information**

We apologize for any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance, visit www.sabreconsumernotice.com or please do not hesitate to contact us at 800 447 0821 (toll free) or +1 503 520 4468 (direct).

Sincerely,

Chief Operating Officer

HISTORIC HOTELS
*of* AMERICA
National Trust *for* Historic Preservation®

<<Mail ID>>
<<First_Name>><<Mid_Name>><<Last_Name>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

<<DATE>>

**NOTICE OF DATA BREACH**

Dear <<First_Name>><<Last_Name>>:

We are writing to you because of an incident that we were recently made aware of by one of our service providers, involving the unauthorized access to your personal information associated with your hotel reservation(s).

We take the privacy and protection of your information 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 the potential misuse of your information.

**What Happened?**

Sabre Hospitality Solutions, a company that facilitates the booking of our reservations either through our member hotels, our call centers, travel agencies, online travel agencies, or similar booking services informed us that an unauthorized party gained access to their SynXis Central Reservations system. We have been told that this unauthorized party could view unencrypted payment card information, as well as certain reservation information, for a subset of hotel reservations processed through their system.

Following an investigation and examination of its forensic evidence, Sabre notified us on or about June 6, 2017 of the incident. Sabre's investigation determined that the unauthorized party first obtained access to certain unencrypted payment card and other reservation information for a subset of hotel reservations processed through their system on August 10, 2016. According to Sabre, the last access to payment card or reservation information was on March 9, 2017.

**What Information Was Involved?**

Based on the information Sabre provided to us, we have reason to believe that the unauthorized party was able to access payment card information for your hotel reservation(s), including cardholder name; card number; card expiration date; and, potentially, your card security code. We have been informed that the unauthorized party was also able, in some cases, to access certain information such as guest name, email, phone number, address, and other information if it was included with your reservation. We have been assured that information such as Social Security, passport, or driver's license numbers were not accessed.

**What We Are Doing**

We are currently working with Sabre to ensure they evaluate and improve their data security processes and we are notifying affected guests and our member hotels of this unfortunate incident. Law enforcement, payment card brands and the major credit reporting agencies have also been notified.

**What You Can Do**

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 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 (typically, between $5.00 and $10.00, depending on your state). Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

You may contact the nationwide credit reporting agencies at:

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

**For More Information**

We apologize for any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance, visit www.sabreconsumernotice.com or please do not hesitate to contact us at 800 472 3981 (toll free) or +1 503 597 7671 (direct).

Sincerely,

Chief Operating Officer