



RETURN MAIL PROCESSING CENTER
PO BOX 6336
PORTLAND, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

We are writing because of an incident that resulted in the unauthorized access to the hotel reservation system of Sabre Hospitality Solutions known as Sabre Hospitality Solutions SynXis Central Reservation system (CRS). Like many other hotels and hospitality companies, CRS may be used to make reservations at our properties, including information associated with your hotel reservation(s) at one of our hotels booked between August 10, 2016 and March 9, 2017. Though the breach was of CRS, not our systems, and you may have already heard of the breach affecting CRS (possibly referencing Sabre or SynXis), we want to provide you with this additional notification beyond what you may have read in the press or received from other third parties out of an abundance of caution. We recommend that you closely review the information provided in this letter for some steps that you may take to protect yourself against potential misuse of your information.

What happened

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

The 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.

What information was involved

The unauthorized party was able to access payment card information in Sabre's CRS system for reservations that include your Sixty Hotels reservation(s), including cardholder name; card number; card expiration date; and, potentially, your card security code. In some cases, the unauthorized party was also able to access certain additional hotel reservation information such as guest name, email, phone number, address, and other information. We have been informed by Sabre Hospitality Solutions that information such as Social Security, passport, or driver's license number was not accessed.

What we are doing

Sabre engaged a leading cybersecurity firm to support its investigation of the breach of its systems. Sabre also notified law enforcement and the payment card brands about this incident. We will continue to work with them and provide any cooperation they need to investigate this incident and help protect you.

What You Can Do

Additional steps you can take to protect yourself from potential identity theft and fraud

1. 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.
2. 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/>

Additional information is also available at the web site of the California Office of Privacy Enforcement and Protection at www.privacy.ca.gov.

If you find that your information has been misused which you believe is as a result of the breach of Sabre's CRS, 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.

3. Place a 90-day Fraud Alert. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file. An initial fraud alert lasts 90 days and tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit reporting companies. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three bureaus will send you your credit report to review, free of charge.

To place a fraud alert on your credit report, contact one of the credit reporting companies (you do not need to contact all of them):

TransUnion
www.transunion.com
Phone: 800-680-7289
P.O. Box 2000
Chester, PA 19016

Equifax
www.equifax.com
Phone: 888-766-0008
P.O. Box 740241
Atlanta, GA 30374

Experian
www.experian.com
Phone: 888-397-3742
P.O. Box 4500
Allen, TX 75013

4. Consider Placing a Credit (Security) Freeze. Also known as a security freeze, this tool prevents others from seeing your credit report and credit score unless you decide to lift the freeze. There is a small fee for placing a freeze, and you must contact each of the credit reporting companies separately. In addition, please note that when a freeze is in place you will have to take additional steps before you can apply for credit or permit others—such as prospective landlords—to view your credit report. You will need to lift the freeze temporarily, either for a specific time or for a specific party. For California residents, the credit reporting companies must lift the freeze within 3 business days, and the fee for lifting the freeze temporarily is \$10 for a date-range lift, or for a lift for a specific creditor. You can find further information about credit freezes at the following website from the California Office of the Attorney General: <https://oag.ca.gov/idtheft/facts/freeze-your-credit>.

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 (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

**Trans Union Security Freeze
Fraud Victim Assistance
Department**
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com
Phone: 888-909-8872

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com
Phone: 800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com
Phone: 888-397-3742

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, provide 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, include 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, include 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 bureaus 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.

This information may be repetitive of what you have already heard in the press or received from Sabre Hospitality Solutions or another user of CRS.

For More Information

As noted, we will continue to work with Sabre Hospitality Solutions and law enforcement agencies. Sabre Hospitality Solutions has not informed us that their reports and notifications have been delayed as a result of any request by law enforcement.

We sincerely regret any inconvenience this compromise of Sabre's CRS has or may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact Sabre Hospitality Solutions at 1-888-721-6305 or 1-503-520-4448 (outside the U.S.).

Regards,

SIXTY Hotels