

JONES DAY

90 SOUTH SEVENTH STREET • SUITE 4950 • MINNEAPOLIS, MINNESOTA 55402
TELEPHONE: +1.612.217.8800 • FACSIMILE: +1.844.345.3178

November 15, 2017

Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RECEIVED
NOV 27 2017
CONSUMER PROTECTION

Re: Sabre Hospitality Solutions Data Security Incident

To Whom May it May Concern:

Pursuant to N.H. R.S.A. 359-C:20, I am writing on behalf of JRK Hotel Group ("JRK") to notify you of a data security incident that occurred on the systems of Sabre Hospitality Solutions ("Sabre"). Sabre is a service provider used to make reservations at JRK hotels. The incident did not affect JRK's systems.

JRK was recently notified of this security incident by Sabre. According to the information we received from Sabre, the incident may have involved unauthorized access to payment card information for hotel reservations, including names, card numbers, card expiration dates, but not card security codes. In some cases, e-mail addresses, telephone numbers and mailing addresses may also have been involved. Information such as Social Security, passport, and driver's license numbers were not accessed. According to Sabre, information within Sabre's system may have been accessed without authorization between August 10, 2016 and March 9, 2017. JRK confirmed that Sabre investigated and remediated the incident with assistance from a digital forensics firm and notified law enforcement and payment card brands in order to prevent fraudulent activity.

We have identified approximately two (2) residents of New Hampshire may have been affected by this issue. It has taken time to determine which individuals were affected. After learning of this incident, JRK worked diligently to identify contact information for affected individuals to provide them with notice of the incident. Sabre has not informed us that their reports and notifications have been delayed as a result of any request by law enforcement. Enclosed for your reference is a copy the notice being sent to New Hampshire residents. JRK is also providing substitute notice through a link to a Sabre microsite, <http://www.sabreconsumernotice.com>.

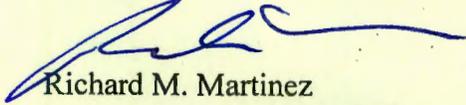
ALKHOBAR • AMSTERDAM • ATLANTA • BEIJING • BOSTON • BRISBANE • BRUSSELS • CHICAGO • CLEVELAND • COLUMBUS • DALLAS
DETROIT • DUBAI • DÜSSELDORF • FRANKFURT • HONG KONG • HOUSTON • IRVINE • JEDDAH • LONDON • LOS ANGELES • MADRID
MEXICO CITY • MIAMI • MILAN • MINNEAPOLIS • MOSCOW • MUNICH • NEW YORK • PARIS • PERTH • PITTSBURGH • RIYADH
SAN DIEGO • SAN FRANCISCO • SÃO PAULO • SHANGHAI • SILICON VALLEY • SINGAPORE • SYDNEY • TAIPEI • TOKYO • WASHINGTON

November 15, 2017

Page 2

Should you have any questions regarding this matter, please do not hesitate to contact me.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Richard M. Martinez", with a long horizontal flourish extending to the right.

Richard M. Martinez

Enclosures



HOTEL
GROUP

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>>

November 15, 2017

Re: Notice of Sabre Data Breach

Dear <<Name1>>:

We are writing because of an incident that resulted in the unauthorized access to the Sabre hotel reservation system, a third party hotel reservations provider. Like many other hotels and hospitality companies, Sabre 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 Sabre, not our systems, we want to provide you with this additional notification beyond what you may have read in the press or received from other 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.

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

What Happened

Sabre facilitates the booking of hotel reservations made by consumers through JRK Hotel Group 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 Sabre. 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.

Please note that the data breach did not involve any systems maintained by our hotels or any information you provided to JRK Hotels.

What Information Was Involved

The unauthorized party was able to access payment card information in the Sabre system for reservations that include your JRK Hotel Group reservation(s), including cardholder name; card number; card expiration date; and, potentially, 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 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 major credit card brands about this incident so they can coordinate with card issuing banks to monitor for fraudulent activity on cards used. 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 a result of the breach of the Sabre system, 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.

If you are a Massachusetts resident, you have the right to obtain a police report in regard to this incident and to file and obtain a copy of a police report if you are a victim of identity theft.

If you are a resident of Iowa, Rhode Island, Maryland, North Carolina, or Oregon, you may contact law enforcement or the Attorney General's Office to report suspected incidents of identity theft or to obtain information about avoiding identity theft:

Office of the Attorney General of Iowa Hoover State Office Building 1305 E. Walnut Street Des Moines, IA 50319 (515) 281-5164 www.iowaattorneygeneral.gov	RI Office of the Attorney General 150 South Main Street Providence, RI 02903 (401) 274-4400 http://www.riag.ri.gov/	Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 (888) 743-0023 www.marylandattorneygeneral.gov	North Carolina Department of Justice Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001 (877) 566-7226 http://www.ncdoj.gov	Oregon Department of Justice 1162 Court Street NE Salem, OR 97301-4096 (503) 378-4400 http://www.doj.state.or.us/
--	---	--	--	---

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.

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 Massachusetts residents, Massachusetts law 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.

If you are a resident of New Mexico, 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 <https://www.consumer.ftc.gov/articles/pdf-0096-faircredit-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. 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.

If you are a resident of Rhode Island, 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 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, 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. 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 written request to each of the three major consumer reporting agencies by regular, certified or overnight mail: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) 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 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. 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.

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>.

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

For More Information

As noted, we will continue to work with Sabre and law enforcement agencies. Sabre 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 has or may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact Sabre at 1-888-721-6305 or 1-503-520-4448 (outside the U.S.).



November 15, 2017

Dear JRK Properties Customers:

Sabre is a leading technology provider to the global travel industry, and counts JRK Properties 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 hotels. 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