BRYAN CAVE

BRYAN CAVE LLP 1155 F Street, N.W. Washington, D.C. 20004-1357
T: 202 508 6000 F: 202 508 6200 bryancave.com

July 6, 2017

Jena Valdetero
Direct: (312) 602-5056
jena.valdetero@bryancave.com

VIA FEDERAL EXPRESS

State of New Hampshire Department of Justice
Office of the Attorney General Joseph Foster
33 Capitol Street
Concord, NH 03301

Re: Voluntary Data Security Breach Notification

To Whom It May Concern:

Halekulani Corporation ("Halekulani"), a client of Bryan Cave LLP, intends to notify two residents of New Hampshire of a criminal cyber-attack involving a third party business partner, Sabre Hospitality Solutions ("Sabre"). Sabre facilitates and processes certain reservations for Halekulani. Halekulani provides this letter as a courtesy as we do not believe notification is required under N.H. Rev. Stat. 359-C:19.

On June 6th, Sabre made Halekulani aware of an attack on Sabre's systems which allowed an unauthorized third party to access Sabre's systems using authorized log-in credentials between August 10, 2016 and March 9, 2017. Sabre reports that it enlisted a leading forensics firm to help in its investigation. Sabre believes that it has stopped the intrusion, identified all reservations that were potentially accessed, and excluded the unauthorized individual from its systems.

The unauthorized party was able to access payment card information for hotel reservation(s), including credit or debit cardholder name; card number; card expiration date; and card security code. In addition, Sabre informed Halekulani that, in certain cases, the guest's name, email, phone number, address, number of adults and children staying at the hotel, and dates of reservation at Halekulani's hotel was also unlawfully accessed.

Sabre has notified the payment card brands of this incident. In addition, Halekulani is notifying potentially affected customers on July 7, 2017 via U.S. mail. An example of the customer message is attached.

If you would like any additional information concerning the above event, please feel free to contact me at your convenience.

Sincerely,

/s/ Jena Valdetero

Jena Valdetero

Attachment

Halekulani
Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

NOTICE OF DATA BREACH

Dear Valued Guest:

Thank you for your patronage of Halekulani.

I am writing to advise you of a security incident involving Sabre Hospitality Solutions, a company which facilitates and processes the booking of reservations for many hotels, either directly through a hotel website or through online travel agencies. Sabre has indicated you had made your reservation through our hotel website or an affiliate online booking source.

Sabre recently notified Halekulani management that there was a breach of Sabre's data network which resulted in unauthorized access to certain confidential information associated with your hotel reservation at Halekulani. Halekulani's computer networks and guest data themselves however were not compromised and as such remain safeguarded and secure.

What Happened?
According to Sabre, confidential payment card and other guest reservation data was unlawfully accessed during the period from August 10, 2016 to March 9, 2017 by someone who used an authorized credential. Your data was accessed as your booking information was on Sabre's server during this period of time.

What Information Was Involved?
The unauthorized party was able to access payment card information for your hotel reservation(s), including credit or debit cardholder name; card number; card expiration date; and card security code. In addition, Sabre informed Halekulani management that, in certain cases, the guest's name, email, phone number, address, number of adults and children staying at the hotel, and dates of reservation at our hotel was also unlawfully accessed.

What We Are Doing
Sabre notified law enforcement and the payment card brands about the security breach of its network and of the confidential data that was accessed. Sabre also retained a payment card industry forensic investigator to investigate this incident. Sabre has established a website with information about the breach (www.sabreconsumernotice.com).

What You Can Do
Under the circumstances, we strongly recommend that you regularly monitor your accounts for any unauthorized activity. If you discover any suspicious or unusual activity on any account, immediately notify your account institution.

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.

For More Information
Additional information about how to protect yourself, including state-specific information, is enclosed. If you have any questions regarding the Sabre data breach or if you desire further information or assistance, please do not hesitate to contact 888-721-6305, 24 hours a day, Monday through Friday.

We sincerely apologize if you experience any inconvenience because of the Sabre data breach. The privacy and protection of our guests' personal information is of the utmost importance to the management of Halekulani, and we are committed to ensuring that Halekulani's own computer networks and guest data are safeguarded and secure.

Sincerely,

Ulrich Krauer

Ulrich Krauer
General Manager
Halekulani

ADDITIONAL WAYS TO COMBAT IDENTITY THEFT

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.

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

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. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

Please see the following page for certain state-specific information.

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.

IF YOU ARE A NORTH CAROLINA RESIDENT:
You may obtain information about preventing identity theft from the North Carolina Attorney General's Office or the Federal Trade Commission. This office can be reached at:

North Carolina Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.gov

IF YOU ARE AN OREGON RESIDENT:
You may contact law enforcement, including the Oregon Attorney General's Office or the Federal Trade Commission to report suspected incidents of identity theft. This office can be reached at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 378-4400
http://www.doj.state.or.us/

Frequently Asked Questions: Unauthorized Access to the Sabre Hospitality Central Reservations System (CRS)

BACKGROUND ON THE INCIDENT

What prompted the investigation?
The investigation began after Sabre became aware of unusual activity on an account credential involving access to hotel reservation data.

What did the credential allow access to?
The unauthorized party was able to access payment card numbers and, in some cases, certain information such as guest name, email, phone number, address, and other information if provided to the CRS. As information such as Social Security, passport, or driver's license number was ***not*** provided, the unauthorized party was not able to obtain this data.

INVESTIGATION RESULTS

What did the investigation reveal?
Sabre's investigation, supported by a leading cybersecurity firm, determined that an unauthorized party:

- obtained access to account credentials that permitted access to a subset of hotel reservations processed through the CRS;
- used the account credentials to view a credit card summary page on the CRS and access payment card information (although Sabre encrypts the data, this credential had the right to see unencrypted card data);
- and the period of access began on August 10, 2016 until it was shut off on March 9, 2017.

Sabre took successful measures to ensure this unauthorized access to the CRS was stopped and is no longer possible.

If a guest's data was accessed, does that mean it was definitely removed by the unauthorized party?
The investigation did not uncover forensic evidence that the unauthorized party removed any information from the CRS, but it is a possibility. For a large percentage of reservations, payment card security codes were never provided to the CRS and accordingly, the security codes would not have been accessible to the unauthorized party. In some other cases, reservations were made using one-time use virtual payment cards.

Was the payment card information that was accessed encrypted?
Although Sabre stores payment information in the reservation in encrypted form, the unauthorized party was able to access the information in unencrypted format by using a credential that had the right to see unencrypted data.

Why was the payment card information unencrypted?
Sabre stores payment information in the CRS in encrypted form. However, payment card information on the credit card summary page is unencrypted so that hotels can access it to process reservations. Such access is highly restricted, but this credential had the right to see unencrypted card data.

Was law enforcement notified? What about the payment card companies?

Sabre notified law enforcement and continue to support their investigation. Sabre also notified the major card brands about this incident and have sent them the affected numbers that were still in the CRS.

SECURITY OF SABRE'S SYSTEMS

How do we know the Sabre systems are secure?

Sabre took successful measures to ensure that the unauthorized access to the CRS was stopped. There is also no indication that any other Sabre systems were affected or accessed by the unauthorized party. This is based on Sabre's internal investigation, as well as the work of their independent experts.

What is Sabre doing to make all of their systems more secure?

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. Consistent with that approach, Sabre also enlists best-in-class external resources to reassure its travel industry customers and the traveling public that Sabre addresses security with the utmost care and expertise.