

July 31, 2017

Jena Valdetero
Direct: (312) 602-5056
jena.valdetero@bryancave.com**RECEIVED****AUG 07 2017****CONSUMER PROTECTION****VIA US MAIL**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:

A client of Bryan Cave LLP, intends to notify forty-eight (48) 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 the hotels identified in the attached exhibit which are operated by our client. We are providing this letter as a courtesy although, based upon the facts of the incident, notification may not be required under N.H. Rev. Stat. 359-C:19.

On June 6th, Sabre made our client aware of an attack 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 has stated, but our client has not been able to independently confirm, that:

- Sabre stopped the intrusion,
- Sabre identified all reservations that were potentially accessed,
- Sabre 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, in some instances, card security code; 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 one or more of the referenced hotels were also unlawfully accessed, and
- Sabre notified the payment card brands of this incident.

Our client is notifying potentially affected customers in early August, 2017 via U.S. mail through a service provider retained by Sabre. 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

Attachments

EXHIBIT

Big Meadows Lodge

Cedar Grove

Explorer Cabins at Yellowstone

Gideon Putnam Hotel

Grant Grove Village

Gray Wolf Inn & Suites

Honey Creek Resort State Park

Kalaloch Lodge

Lewis Mountain Cabins

Peaks of Otter Lodge

Pine Lodge

Rocky Mountain Park Inn

Sea Crest Beach Hotel

Skyland Resort

Tenaya Lodge

The Lodge at Geneva

Trailer Village RV Park

Wheeling Island Hotel

Wuksachi Lodge

Yavapai Lodge

Yellowstone Park Hotel

[DATE]

[CUSTOMER NAME AND ADDRESS]

NOTICE OF DATA BREACH

Dear Valued Guest:

Sabre Hospitality Solutions, which facilitates and processes the booking of reservations for many hotels including [INSERT NAME OF HOTEL], recently, indicated that they experienced a data breach.

While the breach only impacted Sabre and did not compromise the computer networks and guest data at your hotel, we are providing this notification to you as Sabre has indicated that your information may have been impacted. We have enclosed a letter from Sabre that explains the incident, as well as some general information about identity theft.

What Happened?

Sabre indicated that confidential payment card and other guest reservation data from August 10, 2016 to March 9, 2017, that was held in their reservation system was unlawfully accessed by an unauthorized person. They have further indicated that your booking information was on Sabre's server during that period of time, and, as a result, your information may have been at risk. Sabre has not indicated how many individuals were impacted by the breach overall, or how many individuals were impacted from your state.

What Information Was Involved?

Sabre has indicated that the unauthorized party was able to access payment card information, including such information as credit or debit cardholder name, card number, card expiration date and card security code. In addition, 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 the hotel were also unlawfully accessed.

What We Are Doing

Sabre has informed us that they 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).

We asked that Sabre provide you with the attached notice to give you more information about the breach. Although we are not able to independently verify the information therein, we are continuing to discuss with Sabre how the incident happened and to obtain assurances from them of their ongoing security and how they will handle and investigate security incidents like this in the future.

What You Can Do

Under the circumstances, we strongly recommend that you regularly monitor your credit or debit card account statements for any unauthorized activity. If you discover any suspicious or unusual activity on your payment card account, immediately notify your account institution. In addition, be vigilant about any emails that you may receive that claim to be from the hotel or Sabre, particularly any emails that ask you to provide personal information or click on links.

For More Information

Additional information about how to protect yourself, including state-specific information, is enclosed in the attached sheet titled "Additional Information and Resources about Identity Theft." If you have any questions regarding the Sabre data breach or if you desire further information or assistance, Sabre has set up a toll-free hotline which can be reached at 888-721-6305.

We sincerely apologize if you experience any inconvenience because of the Sabre data breach. The privacy and protection of customer information is of the utmost importance to us, and we are committed to working with Sabre to make sure that they continue to take appropriate steps to protect guest data.



June XX, 2017

Dear [Insert Brand] Customers:

Sabre is a leading technology provider to the global travel industry, and counts [Insert Brand] 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

ADDITIONAL INFORMATION AND RESOURCES

ABOUT IDENTITY THEFT

You may find the following general information and resources helpful concerning identity theft.

Federal Trade Commission

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

No Social Security Numbers or driver's license numbers were exposed in this incident, and, as a result, we have no reason to believe that you may be at risk of new account identity theft. As a general matter, it is advisable to regularly monitor your credit reports to see if any new accounts have been opened under your name. 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.

Fraud Alert or Security Freeze on Your Credit Report File

Although no Social Security Numbers or driver's license numbers were exposed in this incident, and, as a result, we have no reason to believe that you may be at risk of new account identity theft, 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.

STATE SPECIFIC INFORMATION

IF YOU ARE AN IOWA RESIDENT:

You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

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

IF YOU ARE A MARYLAND RESIDENT:

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office.

This office can be reached at:

Office of the Attorney General

Consumer Protection Division

200 St. Paul Place

Baltimore, MD 21202

(888) 743-0023

www.marylandattorneygeneral.gov

IF YOU ARE A MASSACHUSETTS RESIDENT:

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

Massachusetts law also 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. 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, Experian, and TransUnion, by regular, certified, or overnight mail or online at the addresses in the enclosed letter.

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, 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, 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, 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 reporting agencies 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.

IF YOU ARE A NEW MEXICO RESIDENT:

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-fair-credit-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. 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.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies using the contact information provided in the enclosed letter.

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 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 apply online or send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided in the enclosed letter.

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. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, 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, payment. Do not send cash through the mail.