

**LEWIS
BRISBOIS
BISGAARD
& SMITH LLP**
ATTORNEYS AT LAW

550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Telephone: 215.977.4100
Fax: 215.977.4101
www.lewisbrisbois.com

STATE OF NH
DEPT OF JUSTICE

2016 JUN 14 AM 11:29

JAMES E. PRENDERGAST
DIRECT DIAL: 215.977.4058
JIM.PRENDERGAST@LEWISBRISBOIS.COM

June 10, 2016

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Mr. Foster:

We represent MEI-GSR, 9550 Firestone Blvd. Suite #105, Downey, CA 90241. MEI-GSR is the owner of the Grand Sierra Resort, and we are writing to notify your office of an incident that may affect the security of personal information relating to certain New Hampshire residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MEI-GSR does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On or around September 29, 2015, the Grand Sierra Resort was contacted by law enforcement regarding an investigation into a potential compromise of payment card information used at food and retail locations at the Grand Sierra Resort. The Grand Sierra Resort immediately began to cooperate with law enforcement and to investigate this matter. Third party forensics investigators were retained to assist the Grand Sierra Resort. Since discovering the compromise, the Grand Sierra Resort has worked closely with law enforcement and its forensics investigators to determine what happened, what information may be at risk and to whom this information may relate. On or around January 11, 2016, these investigators confirmed that certain guest payment card information for cards used at food and retail locations at the Grand Sierra Resort may have been compromised.

The investigation has determined that payment card information used at the Grand Sierra's onsite food and retail locations between February 19, 2014 and March 13, 2014 or March

20, 2015 and August 6, 2015 could be at risk. This includes information like the cardholder's name, credit card number, credit card expiration date, Track 1 data and Track 2 data. Please note that this incident did not affect payment cards used to book or pay for lodging.

Notice to New Hampshire Residents

On April 25, 2016, the Grand Sierra Resort provided substitute notice of this incident to potentially affected customers by posting a notice to its website and issuing a press release to state wide media. Substitute notice was provided substantially the same form as the release attached here as *Exhibit A*. The Grand Sierra Resort was able to work with American Express and use its own records to identify the mailing addresses for some of the potentially impacted customers, which included forty two (42) New Hampshire residents. This process took some time and the Grand Sierra Resort was able to begin providing written notice to those customers the Grand Sierra Resort was able to find address information beginning on June 6, 2016. Written notice was provided in substantially the same form as the letter attached here as *Exhibit B*.

Other Steps Taken and To Be Taken

Upon being contacted by law enforcement, the Grand Sierra began to investigate and to prevent further unauthorized access to customer payment information. The Grand Sierra Resort has enhanced existing security measures to prevent further unauthorized access to customer payment information.

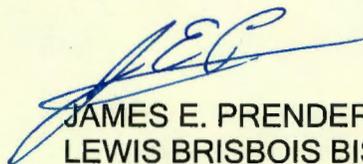
The Grand Sierra Resort is providing potentially impacted customers with guidance on how to protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, state attorney general, and law enforcement to report attempted or actual identity theft and fraud. The Grand Sierra Resort has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. The Grand Sierra Resort is also providing written notice of this incident to other state regulators and the national consumer reporting agencies as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 215-977-4058.

Joseph Foster
June 10, 2016
Page 3

Very truly yours,



JAMES E. PRENDERGAST of
LEWIS BRISBOIS BISGAARD & SMITH LLP

JEP

Exhibit A



April 25, 2016

RE: NOTICE OF DATA BREACH

We are writing to notify guests of an unfortunate situation regarding a data security incident that may have affected the security of certain guest payment card information. Below is information on the incident and resources available to protect potentially impacted guests against identity theft or fraud, should they feel the need to do so.

WHAT HAPPENED? On or around September 29, 2015, the Grand Sierra Resort was contacted by law enforcement regarding an investigation into a potential compromise of payment card information used at food and retail locations at the Grand Sierra Resort. We immediately began to cooperate with law enforcement and to investigate this matter. Third party forensics investigators were retained to assist the Grand Sierra Resort. On or around January 11, 2016, these investigators confirmed that certain guest payment card information for cards used at food and retail locations at the Grand Sierra Resort may have been compromised.

WHAT INFORMATION WAS INVOLVED? The investigation has determined that payment card information used at the Grand Sierra's onsite food and retail locations between February 19, 2014 and March 13, 2014 or March 20, 2015 and August 6, 2015 could be at risk. This includes information like the cardholder's name, credit card number, credit card expiration date, Track 1 data and Track 2 data. **Please note that this incident did not affect payment cards used to book or pay for lodging.**

WHAT WE ARE DOING? Since discovering the compromise, we have worked closely with law enforcement and our forensics investigators to determine what happened, what information may be at risk and to whom this information may relate. Additionally, as part of our ongoing commitment to the security of the personal information in our care, we have worked diligently to enhance existing security measures to prevent further unauthorized access to guest payment card information.

WHAT YOU CAN DO. We encourage potentially impacted guests to review the information below on how to better protect against identity theft or fraud.

FOR MORE INFORMATION. We apologize for any inconvenience and concern this incident causes you. The security of our guests' personal information is one of our highest priorities. Should you have any questions about the content of this notice or ways you can protect yourself from the possibility of identity theft, please call our dedicated hotline at (877) 216-3789 between 9 a.m. and 7 p.m. EST, Monday to Friday. Please use reference number 6216041816 when calling.

ADDITIONAL STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

You may take action directly to further protect against possible identity theft or other financial loss. We encourage you to be vigilant against incidents of identity theft by reviewing your account statements regularly and monitoring your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.



At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
www.transunion.com

In addition to a fraud alert, consumers may place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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.

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 a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place the freeze on all of your credit files.

To find out more on how to place a security freeze, you can contact the credit reporting agencies using the information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
800-685-1111
800-349-9960 (NY Residents)
www.freeze.equifax.com

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

TransUnion LLC
P.O. Box 2000
Chester PA 19022-2000
888-909-8872
freeze.transunion.com

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/idtheft/, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

Exhibit B



June 10, 2016

##B8880-L01-0123456 0001 00000001 *****9-OELZZ 123



SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



RE: NOTICE OF DATA BREACH

Dear Sample A Sample,

We are writing to notify you of an unfortunate situation regarding a data security incident that may have affected the security of certain guest payment card information. We are writing to provide you with information on the incident and resources available to protect against identity theft or fraud, should you feel the need to do so.

WHAT HAPPENED? On or around September 29, 2015, the Grand Sierra Resort was contacted by law enforcement regarding an investigation into a potential compromise of payment card information used at food and retail locations at the Grand Sierra Resort. We immediately began to cooperate with law enforcement and to investigate this matter. Third party forensics investigators were retained to assist the Grand Sierra Resort. On or around January 11, 2016, these investigators confirmed that certain guest payment card information for cards used at food and retail locations at the Grand Sierra Resort may have been compromised.

WHAT INFORMATION WAS INVOLVED? The investigation has determined that payment card information used at the Grand Sierra's onsite food and retail locations between February 19, 2014 and March 13, 2014 or March 20, 2015 and August 6, 2015 could be at risk. This includes information like the cardholder's name, credit card number, credit card expiration date, Track 1 data and Track 2 data. **Please note that this incident did not affect payment cards used to book or pay for lodging.**

WHAT WE ARE DOING. Since discovering the compromise, we have worked closely with law enforcement and our forensics investigators to determine what happened, what information may be at risk and to whom this information may relate. Additionally, as part of our ongoing commitment to the security of the personal information in our care, we have worked diligently to enhance existing security measures to prevent further unauthorized access to guest payment card information.

WHAT YOU CAN DO. We encourage you to review the enclosed information on how to better protect against identity theft or fraud.

FOR MORE INFORMATION. We apologize for any inconvenience and concern this incident causes you. The security of your personal information is one of our highest priorities. Should you have any questions about the content of this letter or ways you can protect yourself from the possibility of identity theft, please call our dedicated hotline at (877) 216-3789 between 9 a.m. and 7 p.m. EST, Monday to Friday. Please use reference number 4843041816 when calling.

0123456



Sincerely,

Rod Luck,
Sr. VP of Information Technology

ADDITIONAL STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

You may take action directly to further protect against possible identity theft or other financial loss. We encourage you to be vigilant against incidents of identity theft by reviewing your account statements regularly and monitoring your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
www.transunion.com

In addition to a fraud alert, consumers may place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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.

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 a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place the freeze on all of your credit files.

To find out more on how to place a security freeze, you can contact the credit reporting agencies using the information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
800-685-1111
800-349-9960 (NY Residents)
www.freeze.equifax.com

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

TransUnion LLC
P.O. Box 2000
Chester, PA 19022-2000
888-909-8872
freeze.transunion.com

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6400, www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.ftc.gov/idtheft/, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.