LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720-292-2052

June 10, 2019

VIA ELECTRONIC SUBMISSION

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110
Email: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald,

We represent Breckenridge Grand Vacations ("BGV") in connection with a recent data security incident, which is described in greater detail below.

1. Nature of the security incident.

In December of 2018, BGV discovered that a thumb drive containing employee information was misplaced while BGV was in the process of changing software providers for its payroll and human resources records. The thumb drive contained full names and Social Security numbers, health insurance plan information, and/or financial institution and account information for some current and former BGV employees. As soon as BGV discovered the incident, BGV conducted an investigation to locate the thumb drive, which was last seen in the BGV office, but the thumb drive was not found. BGV has no evidence that the thumb drive was accessed or acquired by any unauthorized person. Additionally, the information contained on the thumb drive would not have been accessible without a unique company passcode and specific payroll software. However, out of an abundance of caution, BGV took steps to identify each potentially affected individual and provide each notification about the incident and complimentary credit monitoring services thereto.

2. Number of New Hampshire residents affected.

BGV notified two (2) New Hampshire residents regarding this incident. The notification letters were mailed on June 7, 2019. A sample copy of the letter is enclosed.

3. Steps taken relating to the incident.

BGV has taken steps in response to this incident to enhance the security of personal information in its possession in an effort to prevent similar incidents from occurring in the future, including updating its policies and procedures regarding the use of external storage devices for storage or transfer of personal information. In addition, BGV has offered affected individuals 12 months of complimentary credit monitoring and fraud assistance.

4. Contact information.

BGV remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (720) 292-2052, or by e-mail at Alyssa.Watzman@lewisbrisbois.com.

Best regards,

Alyssa Watzman
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure

<<Name 1>> <<Name 2>> <<Date>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

Subject: Notification of Data Security Incident

Dear <<Name1>> <<Name 2>>:

I am writing to inform you of a data security incident that may have affected your personal information. At Breckenridge Grand Vacations ("BGV"), we take the privacy and security of our current and former employees' information very seriously. That is why we are providing you with information about this incident and steps you can take to help protect your personal information.

What Happened? In December of 2018, we discovered that a thumb drive containing employee payroll information was misplaced while we were in the process of changing software providers for BGV payroll and human resources records. We immediately conducted an investigation to locate the thumb drive, which was last seen in the BGV office, but the thumb drive was not found. We have no reason to believe that the thumb drive was accessed or acquired by any unauthorized person. Moreover, the information contained on the thumb drive could not have been accessed without a unique company passcode and specific payroll software. However, out of an abundance of caution, we are notifying you about this incident and providing you with information about steps you can take to help protect your personal information.

What Information Was Involved? The thumb drive may have contained your full name, Social Security number, health insurance plan information, and financial institution and account information (for direct deposit). As stated above, we are not aware of any evidence that the thumb drive has been accessed or acquired without authorization or that any information contained on the thumb drive has been misused, and we are providing you with this letter out of an abundance of caution.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. We have also updated our policies and procedures for the use of external storage devices for storage or transfer of personal information to reduce the risk of a similar incident from occurring in the future. In addition, as a precautionary measure and to safeguard your information from any potential misuse, we are providing you with access to ***Single Bureau Credit Monitoring /Single Bureau Credit Report/Cyber Monitoring**** services at no charge. These services provide you with

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

alerts for twelve (12) months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. The cyber monitoring will review the dark web and alert you if your personally identifiable information is found online. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by **CyberScout** a company that specializes in identity theft education and resolution.

To enroll in Credit Monitoring* services at no charge, please log on to https://www.myidmanager.com and follow the instructions provided. When prompted, please provide the following unique code to receive services: **<<Code Here>>.**

CyberScout is a global leader in risk mitigation and response, and the CyberScout team has extensive experience helping people who have sustained an unintentional exposure of confidential data. For guidance with the CyberScout services, or to obtain additional information about these services, **please call the CyberScout help line *1-800-405-6108*** and supply the fraud specialist with your unique code. Additional information describing your services is included with this letter.

What You Can Do: We encourage you to enroll in the complimentary credit monitoring and identity protection services being offered. You can also follow the recommendations on the following pages to help protect your personal information.

For More Information: Further information about how to protect your personal information appears on the following pages. If you have questions or need assistance, please do not hesitate to call 1-800-405-6108, Monday through Friday, 8:00 a.m. to 5:00 p.m. MT.

We sincerely regret any inconvenience or concern that this matter may cause you and remain dedicated to protecting all information in our systems.

Sincerely,

Nick Doran
Chief Operating Officer
Breckenridge Grand Vacations

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring 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.