Michael Best & Friedrich LLP
Attorneys at Law
Adrienne S. Ehrhardt
T 608.283.0131
E asehrhardt@michaelbest.com

July 10, 2017

Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

Pursuant to N.H. Rev. Stat. § 359-C:20, Great Wolf Resorts, Inc. ("GWR"), through its attorneys Michael Best & Friedrich, LLP, is writing to notify you of an unauthorized access to personal information at GWR's service provider, Sabre GLBL Inc. ("Sabre"), involving 2 New Hampshire residents, of which it is aware. Craig Johnson, General Counsel, Great Wolf Resorts, Inc., (608) 662-4751, cjohnson@greatwolf.com, is the business contact, and Adrienne Ehrhardt, (608) 283-0131, asehrhardt@michaelbest.com, from Michael Best & Friedrich is GWR's attorney contact, assisting GWR with the management of this incident.

By letter dated June 6, 2017, Sabre notified GWR that it had determined that an unauthorized party obtained access to Sabre account credentials that allowed that unauthorized party to view a credit card summary page that included payment card information for various hotel customers, including some GWR customers. Sabre informed GWR that the unauthorized access began approximately August 10, 2016, and ended on or about March 9, 2017, when Sabre was able to stop that access after becoming aware of it. The credit card summary page contained name, address, credit card number, card expiration date, and for a subset of reservations, card security code. Sabre informed GWR that it has engaged a leading cybersecurity firm to investigate the incident and notified law enforcement and the payment card brands of this incident as well. In addition, Sabre has set up a dedicated call center for those potentially affected GWR customers to call with questions regarding this incident. After looking into this incident itself and obtaining additional information from Sabre, GWR has decided to send notifications to the affected residents to inform those individuals of this incident at Sabre in substantially the same form as the document enclosed herewith. These notifications will be emailed or mailed on or about July 19, 2017. Please let us know if you have any questions or would like to discuss further.

Sincerely,

Adrienne Ehrhardt

Adrienne Ehrhardt

Enclosure

041584-0310\21353366.1

[NAME, ADDRESS, LOGO OF COMPANY PROVIDING NOTICE]
[DATE]
[CUSTOMER NAME AND ADDRESS]

NOTICE OF DATA BREACH

Dear Guest:

The privacy and protection of our guests' information is a matter we take very seriously which is why we wanted to alert you to a cyber incident recently reported by Sabre GLBL Inc. ("Sabre").

You may not be familiar with the name Sabre. They developed a travel reservation system used to power the booking functionality for a number of popular third party online travel agencies. This system, called the Hospitality Solutions SynXis Central Reservations System ("CRS"), allows online travel agencies the ability to instantaneously book stays for clients at a number of hotels and resorts around the world, including reservations at Great Wolf Lodge, along with packaged tours, cruise ship and river boat vacations.

What Happened?

Sabre notified us on or about June 6, 2017, that an unauthorized party gained access to Sabre account credentials that permitted unauthorized access to unencrypted payment card information, as well as certain reservation information, for a subset of hotel reservations across numerous travel providers and hotels stored on Sabre's systems and processed through the CRS. This includes a small percentage of our guests who booked a stay at Great Wolf Lodge through a third party online travel agency. Following receipt of the notice, we worked closely with Sabre to gather additional details of the breach and fully understand the potential impact to our guests.

Sabre's investigation determined that the unauthorized party first obtained access to payment card andother reservation information at Sabre on August 10, 2016. The last access to payment card information was on March 9, 2017. The investigation did not uncover forensic evidence that the unauthorized party had removed any information from the system, but it was possible.

What Information Was Involved?

The unauthorized party was able to access Sabre's systems and view payment card information for your hotel reservation(s), including cardholder name; card number; card expiration date; and, potentially, your card security code. The unauthorized party was also able, in some cases, to access certain information such as guest name, email, phone number, address, and other information stored in the Sabre system. **Information such as Social Security, passport, or driver's license number was not accessed.**

What We Are Doing

The privacy of our guests' information is of the utmost importance. We worked with Sabre to obtain reservations records of those guests affected by this incident and have sent out notifications to those potentially compromised. We also set-up a dedicated email address (sabre.information@greatwolf.com) and phone number 888-721-6305 for guests who may have questions about the incident. Sabre engaged a leading

cybersecurity firm to support its investigation. Sabre also notified law enforcement and the payment card brands about this incident.

What You Can Do

You should 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.

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.

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.

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.

You may contact the nationwide credit reporting agencies at:

Equifax P.O. Box 105788 Atlanta, GA 30348 (800) 525-6285 www.equifax.com	Experian P.O. Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19016 (800) 680-7289 www.transunion.com

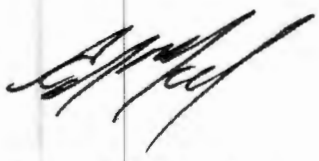
Please see the following page for certain state-specific information.

For More Information

We apologize for any inconvenience caused by this incident. Sabre has set up a call center for consumers who seek additional information about this incident. That number is 888-721-6305.

We are committed to doing what is necessary to protect our guests, so if you have any questions about this incident, please contact me at 608-662-4677 or sabre.information@greatwolf.com.

Howling Regards,



Edward Malinowski
Chief Information Officer
Great Wolf Resorts

IF YOU ARE AN IOWA RESIDENT:
You may contact 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 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. 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 obtain information about preventing identity theft from the Oregon Attorney General's Office. 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