Brownstein Hyatt
Farber Schreck

STATE OF NH
DEPT OF JUSTICE

2015 OCT 13 PM 12: 04

Emily Holmes
Attorney at Law
303.223.1142 tel
303.223.0942 fax
eholmes@bhfs.com

October 6, 2015

VIA FIRST CLASS MAIL

State of New Hampshire
Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301

RE: **Notice of Data Breach**
Client-Matter No. 020009.0008

To Whom it May Concern:

We represent Peppermill Casinos Inc. and are writing to inform you of an information security breach at Peppermill Resort Spa Casino that may have compromised the security, confidentiality or integrity of New Hampshire citizens' credit card information. A copy of the letter sent to affected residents of your state is enclosed.

NATURE OF BREACH & INFORMATION AFFECTED

This security incident relates to the unauthorized and illegal acquisition, by hackers, of certain credit and debit cards used at Peppermill's front desk. The attack was limited to credit or debit transactions between October 12, 2014 and February 16, 2015, and we became aware of the existence, nature and extent of the security incident in late April 2015. However, we delayed notification due to an ongoing investigation by law enforcement.

The unencrypted information potentially compromised by the security incident includes: the name of the card holder, card numbers, expiration dates, and credit card security codes (such as CVV or CVC codes,) but to our knowledge, does not include any other sensitive information.

NUMBER OF RESIDENTS AFFECTED & NOTIFIED

We believe that two (2) residents of the state of New Hampshire were affected by this breach. These residents will be notified via first class U.S. mail, sent on or after the date identified above. Notice was delayed due to (i) an ongoing investigation into the scope of the breach and (ii) an ongoing law enforcement investigation.

STEPS TAKEN TO REMEDY THE BREACH

The integrity of our system was restored following the discovery of the breach. When this breach was discovered we promptly notified law enforcement and the FBI. We have conducted, and recently concluded, a thorough forensic investigation into this security incident in order to determine the full extent

of the breach and number of affected individuals. We continue to work with law enforcement and security researchers to determine the scope of the breach and to find those responsible. Finally, we have designed and implemented new policies and procedures aimed at preventing future security incidents.

CONTACT INFORMATION

If you have any questions or comments, please contact me using the contact information above.

Sincerely,

Emily Holmes

ECH:mcc

Enclosure

020009\0008\13361485.1

Peppermill Casinos, Inc.

CORPORATE OFFICES • 90 WEST GROVE ST. • SUITE 600 • RENO, NEVADA
89509-4003

October 5, 2015

John Doe
9999 Cloverleaf Pl
Castaic, CA 91384-9999

21
30232

Dear John Doe,

We value our customers, and, therefore, protection of our customers' personal information is a significant area of focus in our business. We are writing to inform you of a security incident that may have materially compromised the security, confidentiality or integrity of your credit card information.

This security incident relates to the unauthorized and illegal acquisition, by criminal hackers, of certain credit and debit cards used at Peppermill's front desk. The criminal attack was limited to credit or debit transactions between October 12, 2014 and February 16, 2015, and we became aware of the existence, nature and extent of the security incident in late April 2015. However, we delayed notification due to an ongoing investigation by law enforcement.

The information potentially affected by the security incident includes the name of the card holder, card numbers, expiration dates, and credit card security codes (such as CVV or CVC codes,) but to our knowledge, does not include any other sensitive information. We have conducted, and recently concluded a thorough investigation into this security incident and have implemented new policies and procedures aimed at preventing future security incidents.

Please review your credit and debit card statements and report any suspicious activity to your bank. If you suspect that you are victim of identity theft, you should consider notifying your local law enforcement and the Federal Trade Commission.

We sincerely apologize for any inconvenience or concern this security incident may have caused you. If you have any questions regarding this notice or if you would like more information, please contact us at 1-866-875-4964.

Sincerely,

Scott Evans, Executive Director Customer Service

Resource Guide

Contact Information for Consumer Credit Bureaus:

You may obtain a free copy of your credit report, or request information on how to place a fraud alert or security freeze by contacting any of the national credit bureaus below. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity, regardless whether you suspect any unauthorized activity on your account. The contact information for three major credit bureaus are as follows:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241 Atlanta, GA 30374 1-800-685-1111 www.equifax.com	P.O. Box 2104 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 2000 Chester, PA 19022 1-800-888-4213 www.transunion.com

Contact Information for the Federal Trade Commission

In addition to the credit bureaus above, you may contact or visit the website of the Federal Trade Commission to learn more about how to protect yourself against identity theft, or how to place a fraud alert or security freeze on your account. The contact information for the FTC is as follows:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft
www.identitytheft.gov/

Contact Information for State Government Agencies

Residents of Maryland, North Carolina, Iowa, and California are advised that they may contact their local law enforcement agencies using the following contact information:

Office of the Attorney General of Iowa	**North Carolina Attorney General's Office**
Consumer Protection Division Hoover State Office Building 1305 E. Walnut Street Des Moines, Iowa 50319-0106 Tel: (510) 281-5926 Toll-free: (888) 777-4590	9001 Mail Service Center Raleigh, NC 27699-9001 Telephone: (919) 716-6400 Fax: (919) 716-6750

Maryland Office of the Attorney General	**California Attorney General's Office**
Identity Theft Unit 200 St. Paul Place, 16th Floor Baltimore, MD 21202 Phone: (410) 576-6491 Fax: (410) 576-6566; E-mail: idtheft@oag.state.md.us	California Department of Justice Attn: Office of Privacy Protection P.O. Box 944255 Sacramento, CA 94244-2550 Tel: (916) 322-3360 Toll-free: (800) 952-5255 https://oag.ca.gov/idtheft

How to Place a Fraud Alert on your Account

To protect yourself from the possibility of identity theft or other fraud, you may place a fraud alert on your credit file. The fraud alert helps to prevent someone else from obtaining credit in your name. If you have a fraud alert on your credit file, creditors will contact you and verify your identity before they open any new accounts or change your existing accounts, but it should not affect your credit score or your ability to obtain new credit (although it may cause a delay in any applications or approvals). As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts, so you do not need to place alerts with more than one of the credit bureaus. To place a fraud alert, go to any of the following links and complete the requested steps:

Experian: https://www.experian.com/fraud/center.html

Equifax: https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

Transunion: http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page

How to Place a Security Freeze on Your Account

If you wish to take more extensive measures to prevent new credit being opened in your name, you may consider placing a security freeze on your credit file. You should only place a security freeze if you want to prevent most parties from obtaining your credit report and prevent all credit, loans and related services from being approved in your name without your consent. Please consider that this may also impact or delay your ability to obtain certain government services, rental housing, employment, cell phone plans, insurance, utilities, and many more aspects of your life.

You will need to apply for a security freeze separately with each of the credit bureaus. The requirements to obtain a security freeze vary depending on your state of residence, and you may be required to pay a fee, provide your name and social security number, copies of important identification records (including a list of addresses, copies of government issued IDs, and/or utility bills), provide an incident report if you are a victim of identity theft, or take other measures as described on the credit bureaus' websites. You may need to follow these steps for each individual (such as a spouse or dependent) who will request a security freeze. You can find more information regarding

a security freeze at the following links, or by calling each of the credit bureaus at the numbers listed in this notification letter:

Experian: https://www.experian.com/consumer/security_freeze.html

Equifax: https://www.freeze.equifax.com

Transunion: http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page