



October 1, 2012

Attorney General Michael A. Delaney
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Great River Entertainment

Dear Attorney General Delaney:

We are writing to notify you of a data security event that compromised the security of personal information. Great River Entertainment, LLC ("GRE"), 3001 Winegard Drive, Burlington, Iowa 52601, the entertainment company which includes the Catfish Bend Inn and Spa, Catfish Bend Casino, Fun City and Pzazz Resort Hotel and Event Center, in Burlington, Iowa, is informing your office of pertinent facts that are known at this time related to one of its payment application systems becoming infected by malware of unknown origin. This infection resulted in a potential compromise of credit card information of individuals who patronized these establishments between August and November, 2011 and utilized credit or debit cards to pay for goods and services. Upon discovery of the infection, GRE retained independent security and forensic investigators Security Metrics to determine the extent of the breach and to identify those individuals that may have potentially been affected as a result. GRE's investigation is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, GRE does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Security Event

GRE was notified in November of 2011 that patrons utilizing credit or debit cards for payments for goods and services at some of its establishments between August and November of 2011 were experiencing suspicious card activity. Once notified of the suspicious activity, GRE instructed its payment application system software contractor to update the software and change the system password, and also retained computer security investigation firm Security Metrics to perform a forensic investigation of the system. Security Metrics confirmed on or about March 1, 2012 that a payment application system at one of its establishments had become infected by malware of unknown origin, thus resulting in the potential compromise of patrons' credit and debit card information.

Notice to New Hampshire Residents

Because the payment application system does not retain cardholder names, GRE is unable to identify each affected individual and, instead, has notified Visa, MasterCard, Discover, and American Express of the incident. American Express has advised that its population of affected cardholders includes residents of New Hampshire, and notice to these residents was sent by a third-party vendor of American Express *via* regular mail in substantially the same form as *Exhibit A* on or about September 15, 2012.

Other Steps Taken and To Be Taken

As discussed above, GRE retained forensic computer experts to perform an investigation into the payment application system compromise. GRE also retained legal counsel specializing in data breach response. GRE provided notification to the Missouri Attorney General, and is providing notice to other state regulators as well. The three national credit reporting agencies were also notified.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact our data privacy counsel, James E. Prendergast or Jennifer A. Coughlin, of the law firm Nelson, Levine, de Luca & Hamilton, at 215-358-5087.

Sincerely,



Jerry Baum
Chief Operating Officer
Great River Entertainment, LLC

Re: Great River Entertainment, LLC

Dear :

We are writing to notify you of a data security event that compromised the security of personal information. Great River Entertainment, LLC ("GRE"), 3001 Winegard Drive, Burlington, Iowa 52601, the entertainment company which includes the Catfish Bend Inn and Spa, Catfish Bend Casino, Fun City and Pzazz Resort Hotel and Event Center, in Burlington, Iowa, is informing your office of pertinent facts that are known at this time related to one of its payment application

systems becoming infected by malware of unknown origin. This infection resulted in a potential compromise of credit card information of individuals who patronized these establishments between August and November, 2011 and utilized credit or debit cards to pay for goods and services. Upon discovery of the infection, GRE retained independent security and forensic investigators Security Metrics to determine the extent of the breach and to identify those individuals that may have potentially been affected as a result. GRE's investigation is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, GRE does not waive any rights or defenses regarding the applicability of Missouri law or personal jurisdiction.

Nature of the Security Event

GRE was notified in November of 2011 that patrons utilizing credit or debit cards for payments for goods and services at some of its establishments between August and November of 2011 were experiencing suspicious card activity. Once notified of the suspicious activity, GRE instructed its payment application system software contractor to update the software and change the system password, and also retained computer security investigation firm Security Metrics to perform a forensic investigation of the system. Security Metrics confirmed on or about March 1, 2012 that a payment application system at one of its establishments had become infected by malware of unknown origin, thus resulting in the potential compromise of patrons' credit and debit card information.

Notice to Missouri Residents

Because the payment application system does not retain cardholder names, GRE is unable to identify each affected individual and, instead, has notified Visa, MasterCard, Discover, and American Express of the incident. GRE is publishing notice of the potential data breach on its website, and has also published notice in the Columbia Missourian (MO), Cedar Rapids Gazette (IA), Davenport Quad City Times (IA), Des Moines Register (IA), Peoria Journal Star (IL), Rockford Register Star (IL), and Springfield State Register (IL). A copy of the website statement and media notice is attached to this letter as *Exhibit A*.

Other Steps Taken and To Be Taken

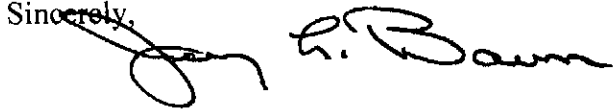
As discussed above, GRE retained forensic computer experts to perform an investigation into the payment application system compromise. GRE also retained legal counsel specializing in data breach response.

Contact Information

New Hampshire Office of Attorney General
October __, 2012
Page 4

Should you have any questions regarding this notification or other aspects of the data security event, please contact our data privacy counsel, James E. Prendergast or Jennifer A. Coughlin, of the law firm Nelson, Levine, de Luca & Hamilton, at 215-358-5087.

Sincerely,

A handwritten signature in black ink, appearing to read "Jerry Baum". The signature is written in a cursive style with a large, looping initial "J".

Jerry Baum
Chief Operating Officer
Great River Entertainment, LLC

Exhibit A

Great River Entertainment, LLC
P.O. Box 727
3001 Winegard Drive
Burlington, Iowa 52601

September 14, 2012

JOHN DOE
1234 MAIN STREET
EL SEGUNDO, CA 90245-3259

Dear John Doe,

We are writing today with important information that affects you.

This information relates to Great River Entertainment, the recreation and entertainment complex in Burlington, Iowa, which includes Catfish Bend Inn and Casino, Fun City and Pzazz Resort Hotel and Event Center.

We are writing to inform you that your American Express credit card information (including your name, credit card number and expiration date) may have been compromised by computer hackers who infiltrated the computer system security that processes food service payments at one or more Great River Entertainment facilities sometime between August 25, 2011 and November 20, 2011. While we recognize that a considerable amount of time has passed since then, the data breach was not confirmed until April 2012. Great River has been working with independent security and forensics investigators to determine the extent of the breach and identify those individuals that may have potentially been affected as a result.

We encourage you to review your American Express account statements from the past year. If you discover a transaction you did not make at our establishment that you believe is fraudulent, please contact us immediately by calling **1-888-414-8020** and provide reference number **9876080812**. Otherwise, you should remain vigilant over the next twelve months and report suspicious activity to American Express.

We want to assure you that this matter is being taken very seriously. The privacy and security of our guests' personal information is one of Great River's highest priorities. The company has taken a series of steps to ensure that this does not happen again by changing all relevant computer passwords, updating software, and increased monitoring of traffic on its servers.

To protect against possible identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports, for at least the next twelve to twenty-four months. Specific steps you can take to protect against the possibility of identity theft include closely monitoring your financial statements for any unusual activity and notifying your credit card company of this notice. 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 (877) 322-8228.

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. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. 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 2104
Allen, TX 75013
888-397-3742
www.experian.com

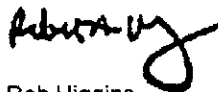
TransUnion
P.O. Box 6790
Fullerton, CA 92834
800-680-7289
www.Transunion.com

To further educate yourself on identify theft and the steps you can take to avoid identity theft, you may contact the Federal Trade Commission. They can be reached at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, or at www.ftc.gov/bcp/edu/microsites/idtheft/ or 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. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; telephone: (919) 716-6400; or www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; telephone: (888) 743-0023; or www.oag.state.md.us.

We again regret any inconvenience or concern that this matter may have caused you. If you have any questions, please contact us Monday - Friday from 8:00 a.m. - 5:00 p.m. CST by calling 1-888-414-8020 and providing reference number 9876080812.

Sincerely,



Rob Higgins
General Manager