

RECEIVED

BakerHostetler

16 MAR -1 AM 10:59
CONSUMER PROTECTION DIV.

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

William R. Daugherty
direct dial: 713.646.1321
wdaugherty@bakerlaw.com

February 29, 2016

**VIA E-MAIL (CONSUMER@IOWA.GOV)
AND OVERNIGHT MAIL**

Office of the Attorney General of Iowa
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut Street
Des Moines IA 50319

Re: Incident Notification

Dear Sir or Madam:

Our clients, Landry's, Inc., Golden Nugget Atlantic City, LLC, Golden Nugget Lake Charles, LLC, GNL Corp., GNLV Corp., and Riverboat Corporation of Mississippi (collectively "the Companies"), understand the importance of protecting payment card information. On December 3, 2015, the Companies received a report from their payment card processor of suspicious activity regarding payment cards that had been used legitimately at some of their locations. The Companies immediately began an investigation and hired a leading cyber security firm to examine their payment card system. The Companies also contacted the payment card networks and law enforcement about the incident.

Findings from the investigation show that criminal attackers were able to install a program on payment card processing devices at certain of the Companies' restaurants, food and beverage outlets, spas, entertainment destinations, and managed properties. The program was designed to search for data from the magnetic stripe of payment cards that had been swiped (cardholder name, card number, expiration date and internal verification code) as the data was being routed through affected systems. Locations were affected at different times during one or both of the following periods: from May 4, 2014 through March 15, 2015 and from May 5, 2015 through December 3, 2015. In addition, the at-risk timeframe for a small percentage of locations includes the period from March 16, 2015 through May 4, 2015.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

On January 29, 2016, the Companies provided substitute notification to affected individuals by posting a statement on their websites and issuing a press release in substantially the same form as the documents enclosed herewith. The list of the affected locations and respective at-risk timeframes was posted with the substitute notification. Notification was not provided to your office at that time because none of the affected locations are in Iowa.

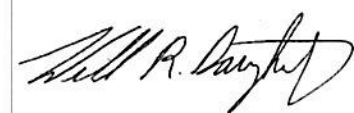
Since then, the Companies have been diligently working to identify those customers that used a payment card at an affected location during the location's at-risk window and for whom the Companies can match the cardholder to a physical address or email address. Now that the Companies have completed the identification and matching process, beginning on February 29, 2016, letters will be sent by first-class mail to 77 Iowa residents in accordance with Iowa Code §715C.1 in substantially the same form as the document enclosed herewith. Notice is being provided as expeditiously as practicable and without unreasonable delay.

The Companies have established a dedicated call center that potentially affected individuals can contact with questions. The Companies are also recommending that potentially affected individuals remain vigilant by reviewing their account statements and credit reports for unauthorized activity.

In addition, the Companies have implemented enhanced security measures, including end-to-end encryption, to prevent a similar issue from occurring in the future, and the Companies continue to support law enforcement's investigation. The Companies also have provided the payment card networks with a list of the affected locations and the respective at-risk windows so that the card issuers can be made aware and initiate heightened monitoring of accounts associated with the potentially affected cards.

Please do not hesitate to contact me if you have any questions regarding this matter.

Best regards,



William R. Daugherty
Counsel

Enclosure



February 29, 2016

«Sack and Pack Numbers» «Presort Sequence» «OEL»
«NAME»
«ADDRESS»
«CSZ»

Dear «FIRST NAME» «LAST NAME»,

Landry's, Inc. and Golden Nugget Hotels and Casinos value the relationship we have with our customers and understand the importance of protecting payment card information. We are writing to inform you about an incident that may involve some of your payment card information.

In early December, we received a report of suspicious activity regarding payment cards that had been legitimately used in some of our locations, and we immediately launched an investigation. We also hired a leading cyber security firm to examine our payment card systems, implemented advanced payment processing solutions, and have been working with the payment card networks and law enforcement.

Findings from the investigation show that criminal attackers were able to install a program on payment card processing devices at certain of our restaurants, food and beverage outlets, spas, entertainment destinations, and managed properties. The program was designed to search for data from the magnetic stripe of payment cards that had been swiped (cardholder name, card number, expiration date and internal verification code) as the data was being routed through affected systems. Locations were affected at different times during one or both of the following periods: from May 4, 2014 through March 15, 2015 and from May 5, 2015 through December 3, 2015. In addition, the at-risk timeframe for a small percentage of locations includes the period from March 16, 2015 through May 4, 2015. Our records show that you used a payment card ending in

Last 4 digits at an affected location during the location's at-risk window. For a list of all of our restaurants, hotels, casinos, entertainment destinations, and managed properties, please visit www.landrysinc.com. For a list of only the affected locations and respective at-risk timeframes, please visit www.landrysinc.com/protectingourcustomers.

Enhanced security measures, including end-to-end encryption, have been implemented to prevent a similar issue from occurring in the future, and we continue to support law enforcement's investigation. We are also working closely with the payment card networks to identify potentially affected cards so that the card issuers can be made aware and initiate heightened monitoring of those accounts.

We recommend that you remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the attachment to this letter for additional steps you may take to protect your information.

Landry's and Golden Nugget regret any inconvenience or concern this may have caused. If you have any questions, please visit www.landrysinc.com/protectingourcustomers or call (877) 238-2151 (U.S. and Canada), Monday thru Friday from 9:00 am to 7:00 pm EST.

Sincerely,

Loti Kittle
Chief Technology Officer

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740256, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. Contact information for the Federal Trade Commission 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

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.