LANDRY'S AND GOLDEN NUGGET COMPLETE INVESTIGATION AND REPORT ON PAYMENT CARD INCIDENT

January 29, 2015

California Residents, please view here

Landry's, Inc. and Golden Nugget Hotels and Casinos (collectively "the Companies") value the relationship we have with our customers. Because we understand the importance of protecting payment card information, we have been working tirelessly to complete the previously announced payment card investigation. The investigation began immediately after we received a report in early December of suspicious activity regarding cards that had been legitimately used in some of our locations. We 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. To view all of our restaurants, hotels, casinos, entertainment destinations, and managed properties, click here. For a list of only the affected locations and respective at-risk timeframes, click here.

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. For those customers we can identify as having used their card at an affected location during that location's at-risk window and for whom we have a mailing address or e-mail address, we will be mailing them a letter or sending them an e-mail.

If you used a payment card at an affected location during its at-risk window, 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 section that follows this notice 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 call (877) 238-2151 (U.S. and Canada), Monday thru Friday from 9:00 am to 7:00 pm EST.

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 19022-2000, www.transunion.com, 1-800-916-8800

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.

If you are a resident of Maryland, you may contact the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

If you are a resident of Massachusetts, note that pursuant to Massachusetts law, you have the right to obtain a copy of any police report.

Massachusetts law also allows consumers to request a security freeze. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. 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 fee for placing a security freeze on a credit report is $5.00. If you are a victim of identity theft and submit a valid investigative report or complaint with a law enforcement agency, the fee will be waived. In all other instances, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. If you have not been a victim of identity theft, you will need to include payment to the credit reporting agency to place, lift, or remove a security freeze by check, money order, or credit card.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

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 19022-2000,www.transunion.com, 1-800-680-7289

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

If you are a resident of North Carolina, you may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400.

If you are a resident of West Virginia, you also have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. 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. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies 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 19022-2000, www.transunion.com, 1-800-680-7289

As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in 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. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft/.

You may also 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 have a right to place a security freeze on your credit report pursuant to West Virginia law. 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, within five business days you will be provided a unique personal identification number ("PIN") or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

(1) The unique personal identification number ("PIN") or password provided by the consumer reporting agency;
(2) Proper identification to verify your identity; and
(3) The period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request.

A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.

If you are actively seeking credit, 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, a few days before actually applying for new credit.

LANDRY'S AND GOLDEN NUGGET COMPLETE INVESTIGATION AND REPORT ON PAYMENT CARD INCIDENT

Houston, TX –January 29, 2016: Landry's, Inc. and Golden Nugget Hotels and Casinos (collectively "the Companies") value the relationship they have with their customers. Because the Companies understand the importance of protecting payment card information, they have been working tirelessly to complete the previously announced payment card investigation. The investigation began immediately after the Companies received a report of suspicious activity regarding cards that had been legitimately used at some of their locations. The Companies hired a leading cyber security firm to examine their payment card systems, implemented advance 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 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. The list of affected locations and respective at-risk timeframes is available at 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 the Companies continue to support law enforcement's investigation. The Companies 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. For those customers the Companies can identify as having used their card at an affected location during that location's at-risk timeframe and for whom the Companies have a mailing address or e-mail address, the Companies will be mailing them a letter or sending them an e-mail.

Customers that used a payment card at an affected location during its at-risk window should remain vigilant to the possibility of fraud by reviewing their payment card statements for any unauthorized activity. Customers should immediately report any unauthorized charges to their 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 the payment card.

Landry's and Golden Nugget regret any inconvenience or concern this may have caused. Customers with questions can call (877) 238-2151 (U.S. and Canada), Monday thru Friday from 9:00 am to 7:00 pm EST.

About Landry's and Golden Nugget

Landry's and Golden Nugget are multinational, diversified restaurant, hospitality, gaming, and entertainment companies based in Houston, Texas. In the aggregate, they operate, own or manage more than 500 high-end and casual dining establishments around the world, including well-known concepts, such as Landry's Seafood, Bubba Gump Shrimp Co., Rainforest Cafe, Morton's The Steakhouse, The Oceanaire, McCormick & Schmick's Seafood, Mitchell's Fish Market, Chart House, Saltgrass Steak House, Claim Jumper, and Mastro's Restaurants. They also operate a group of signature restaurants, including Vic & Anthony's, Grotto, Willie G's, and others. The gaming group includes the renowned Golden Nugget Hotel and Casino concept, with locations in Las Vegas and Laughlin, NV, Atlantic City, NJ, Biloxi, MS, and Lake Charles, LA. The entertainment and hospitality divisions include some managed locations and encompass popular destinations, including the Galveston Island Historic Pleasure Pier, Kemah Boardwalk, Aquarium Restaurants, and other exciting attractions, coupled with deluxe accommodations throughout the Houston and Galveston area, including the Westin Hotel in downtown Houston, the Kemah Boardwalk Inn and luxurious San Luis Resort, as well as the Galveston Island Convention Center, Galveston Island Hilton and Holiday Inn all located on Galveston Island.

CONTACT: Steven L. Scheinthal, Executive Vice President & General Counsel or Richard H. Liem, Executive Vice President & CFO, +1-713-850-1010

LANDRY'S
DINING · HOSPITALITY · ENTERTAINMENT · GAMING

GOLDEN NUGGET

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,

Lori Kittle

Lori 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.