MULLEN COUGHLIN

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.legal

1275 Drummers Lane, Suite 302
Wayne, PA 19087

November 21, 2016

INTENDED FOR ADDRESSEE(S) ONLY

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Notice of Data Event

Dear Sir or Madam:

We represent Island Hotel Company Limited, which operates the Atlantis, Paradise Island (the "Resort"), One Casino Drive, Paradise Island, Bahamas and are writing to notify your office of an incident that may affect the security of payment card information relating to certain Washington residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the Resort does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

Nature of the Data Event

The Resort began investigating unusual activity after receiving reports from its credit card processor. The Resort immediately began working with third-party forensic experts to investigate these reports and to identify any signs of compromise on its computer systems. On October 21, 2016, the Resort discovered suspicious files on its computer systems that indicated a potential compromise of customers' debit and credit card data for some credit and debit cards used at food and beverage and retail locations at the Resort.

Since that time, the Resort has been working with third-party forensic investigators to determine what happened and what information was affected. The Resort has confirmed that malware may have captured data from some credit and debit cards used at food and beverage and retail locations at the Resort. The Resort has removed the malware at issue to contain this incident and implemented additional procedures in an effort to prevent any further unauthorized access to customers' credit and debit card information. This incident did not affect credit and debit cards used to make or pay for hotel reservations or purchases made by guests who charged their food and beverage or retail purchases back to their room.

Notice to Washington Residents

Through the ongoing third-party forensic investigations, the Resort confirmed that malware may have captured credit and debit card data from some credit and debit cards used at its food and beverage and retail locations at the resort between March 9, 2016 and October 22, 2016. The information at risk as a result of this event for credit and debit cards used at the affected food and beverage and retail locations includes the card number, expiration date, CVV and in some instances, cardholder name. The Resort is unable to determine, however, which specific customer's credit and debit card information may have been stolen. Further, the Resort does not have sufficient contact information for customers who may potentially be affected by this incident. Therefore, the Resort is unable to determine the precise number of Washington residents impacted by this incident or provide written notice of this event to these individuals. The Resort is providing substitute notice to those Washington residents impacted by this incident by issuing a press release to prominent media outlets serving Washington on November 21, 2016 and by conspicuously posting a link to a copy of this press release on the homepage of its websites. The press release issued by the Resort relating to this matter is attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

The Resort has established a dedicated hotline for customers to contact with questions or concerns regarding this incident. Additionally, the Resort is providing potentially impacted customers with helpful information on how to protect against identity theft and fraud, including how to place a fraud alert and security freeze on one's credit file, the contact information for the national consumer reporting agencies, how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, state attorney general, and law enforcement to report attempted or actual identity theft and fraud. The Resort is also providing written notice of this incident to other state regulators and the national consumer reporting agencies as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL

EXHIBIT A

Atlantis, Paradise Island Provides Notice of Data Security Incident

Paradise Island, Bahamas, November 21, 2016 – Atlantis, Paradise Island (the "Resort") today announced that a recent data security incident may have compromised the security of payment information of some customers who used debit or credit cards at food and beverage and retail locations at the Resort between March 9, 2016 and October 22, 2016. Customers can now safely use their credit and debit cards at the food and beverage and retail locations at the Resort. This incident did not affect credit and debit cards used to make or pay for hotel reservations or purchases made by guests who charged their food and beverage or retail purchases back to their room.

What Happened? The Resort began investigating unusual activity after receiving reports from its credit card processor. The Resort immediately began working with third-party forensic experts to investigate these reports and to identify any signs of compromise on its computer systems. On October 21, 2016, the Resort discovered suspicious files on its computer systems that indicated a potential compromise of customers' credit and debit card data for some credit and debit cards used at food and beverage and retail locations at the resort.

Since that time, the Resort has been working with third-party forensic investigators to determine what happened and what information was affected. The Resort has confirmed that malware may have captured data from some credit and debit cards used at food and beverage and retail locations at the Resort. The Resort has removed the malware at issue to contain this incident and implemented additional procedures in an effort to prevent any further unauthorized access to customers' credit and debit card information. This incident did not affect credit and debit cards used to make or pay for hotel reservations or purchases made by guests who charged their food and beverage or retail purchases back to their room.

What Information Was Involved? Through the ongoing third-party forensic investigations, the Resort confirmed that malware may have captured credit and debit card data from some credit and debit cards used at food and beverage and retail locations between March 9, 2016 and October 22, 2016. The information at risk as a result of this event for credit or debit cards used at the impacted locations includes the card number, expiration date, CVV and in some instances, cardholder name. This incident did not involve customers' Social Security numbers as this information is never collected by the Resort. This incident did not involve customers' PIN numbers, either.

What We Are Doing. "The Resort takes the security of our customers' information extremely seriously, and we apologize for the inconvenience this incident may have caused our customers," Howard C. Karawan, President and Managing Director of Atlantis, Paradise Island, stated. Mr. Karawan expanded, "We continue to work with third-party forensic investigators to ensure the security of our systems on behalf of our customers and would like to take this opportunity to remind customers to remain vigilant against fraud by reviewing their financial account statements regularly and reporting any suspicious activity."

For More Information. The Resort has established a dedicated assistance line for individuals seeking additional information regarding this incident. Customers can call (877) 223-3689,

Monday through Friday (excluding U.S. holidays), 9 a.m. to 7 p.m. EST and provide reference number 1141111816 when calling. Customers that live in a country that does not support toll free numbers in the North American Numbering Plan, please phone 1-814-201-3667, 9 a.m. to 7 p.m. EST, Monday through Friday (excluding U.S. holidays). Customers can also find information on this incident and what they can do to better protect against fraud and identity theft at www.atlantisbahamas.com.

What You Can Do. The Resort encourages all customers to remain vigilant against identity theft by reviewing their financial account statements regularly and monitoring their credit reports for suspicious activity. Customers should immediately report any unauthorized charges to their card issuer. The phone number to call is usually on the back of the credit or debit card. Under U.S. law, individuals over the age of 18 are entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Customers may also contact the three major credit bureaus directly to request a free copy of their credit report.

The Resort encourages customers who believe they may be affected by this incident to take additional action to further protect against possible identity theft or other financial loss. At no charge, customers can have these credit bureaus place a "fraud alert" on their file, alerting creditors to take additional steps to verify their identity prior to granting credit in their name. Note, however, that because it tells creditors to follow certain procedures to protect the customer, a fraud alert may also delay customers' ability to obtain credit while the agency verifies their identity. As soon as one credit bureau confirms a customer's fraud alert, the others are notified to place fraud alerts on the customer's file. Should customers wish to place a fraud alert or have any questions regarding their credit reports, they may contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Customers may also place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a customer's credit report without the consumer's written authorization. However, customers should be aware that placing a security freeze on their credit reports may delay, interfere with or prevent the timely approval of any requests they make for new loans, credit mortgages, employment, housing, or other services. If a customer has been a victim of identity theft and provides a credit reporting agency with a valid police report, the agency cannot charge the customer to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge a fee to place, temporarily lift or permanently remove a security freeze. Customers will need to place security freezes separately with each of the three major credit bureaus listed above if they wish to place a freeze on all of their credit files. To find out more about how to place a security freeze, customers can contact the credit reporting agencies using the information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents please call 1-800-349-9960)
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion Fraud Victim Assistance
P.O. Box 2000
Chester, PA 19022
Fraud Division
1-888-909-8872
www.transunion.com/credit-freeze/place-credit-freeze

Customers can further educate themselves regarding identity theft, fraud alerts and the steps they can take to protect themselves, by contacting the Federal Trade Commission or their state attorney general. The Federal Trade Commission can be reached at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.ftc.gov/idtheft/, 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 the Commission. Customers can obtain further information on how to file such a complaint by way of the contact information listed above. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. An unknown number of Rhode Island residents may be impacted by this incident. Customers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, customers will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed as a result of a law enforcement investigation.