OLYMPIA HOTEL MANAGEMENT

August 21, 2015

Attorney General Tom Miller
Consumer Protection Division
Attorney General's Office
Attn: Security Breach Notification
Hoover State Office Bldg.
1305 E. Walnut Street
Des Moines, IA 50319

Re: Brunswick Hotel & Tavern – Notice of Data Security Incident Affecting 5 Iowa Residents

Dear Attorney General Miller:

Olympia Hotel Management, LLC ("Olympia," "we", "us"), manager of the Brunswick Hotel & Tavern located at 4 Noble Street, Brunswick, Maine, is writing to notify you of a data security incident that we believe may have compromised the security of 5 Iowa residents' personal information. Based on information made available to us on August 12, 2015, it appears that keylogging malware was placed on the Brunswick Hotel's computer network by unknown individuals and may have resulted in unauthorized access to the personal information of certain guests at the Brunswick Hotel. Below we have provided a more detailed account of the pertinent facts that are known to us at this time.

Nature of the Data Security Incident

In late June, we received an inquiry from a group of three guests about fraudulent credit card charges that occurred after their stay at the Brunswick Hotel. We promptly requested an on-site visit from our network services vendor, but that vendor's scan of our systems did not reveal any malware. After receiving two additional inquiries in July, we elected to review our systems again using a different resource. This second review did reveal evidence of malware, and we promptly performed malware removal scans, thereby ending the immediate threat. Shortly thereafter, we also retained third-party computer forensic experts Verizon Business Network Services, Inc. ("Verizon"), a leading cybersecurity and investigations company, to help us further examine the nature of the detected malware and identify what information on the Brunswick Hotel's network, if any, may have been exposed as a result of the malware. In addition, we retained privacy and data security legal counsel to assist in the ongoing investigation of, and response to, the incident.

Based on Verizon's thorough forensic investigation of our systems, it appears that one of the front desk computers at the Brunswick Hotel was infected with sophisticated malware, known as AlienSpy, designed to capture and exfiltrate payment card information that was typed or swiped into that system while avoiding detection by anti-virus software. Based on forensic investigation results, Verizon has determined that the malware may have been active on or between November 29, 2014 and July 21, 2015 (the "Affected Period") and that the keylogging function of the malware detected guest names and payment card information. To date, Verizon has not found any conclusive evidence that this information was exfiltrated from the system but also cannot conclusively confirm that no information was exfiltrated. As a result, we are taking the conservative view that all guests at the Brunswick Hotel

whose name and payment card information was typed or swiped into the infected front desk terminal during the Affected Period may be at risk and are notifying such guests accordingly.

Notice to Iowa Residents

As stated above, we are notifying all guests whose name and payment card information was typed or swiped into the infected front desk terminal during the Affected Period, including 5 Iowa residents. These state residents will be sent written notice of the data security incident on or around August 28, 2015 in substantially the same form as the sample notice attached to this letter as **Exhibit A.**

Please note that we do not yet have complete contact information for a small number of guests who reserved through third party sources. We are working diligently to obtain this information, and, if we determine that additional Iowa residents are among this group, we will send out subsequent letters. However, to avoid delay we are taking action now with respect to those residents for whom we already have contact information.

Other Steps Taken/To Be Taken

In addition to providing written notification to potentially affected individuals as described above, we will offer each of those individuals one year of credit monitoring through Experian, at no cost to those individuals. We continue to work with independent, third-party computer forensic experts and privacy and data security legal counsel to help us further evaluate the situation and to take appropriate action. We have also notified and are working with our payment card vendors to limit the risk to customers of fraudulent card charges, and will be sending written notice to the major credit reporting agencies. Finally, we are providing notice of this data security incident to regulators in other states whose residents may be affected.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security incident, please contact our privacy and data security legal counsel, Peter Guffin (207-791-1199 / pguffin@pierceatwood.com) or Kyle Glover (207-791-1289 / kglover@pierceatwood.com), of the law firm of Pierce Atwood LLP, located at 254 Commercial Street, Portland, ME 04101.

Sincerely,

Daniel J. Flaherty
Olympia Hotel Management, LLC
Manager of the Brunswick Hotel & Tavern

OLYMPIA HOTEL MANAGEMENT

August 21, 2015
«title»«firstname» «lastname»
«address1»
«address2»
«city», «stateprov» «postalcode»

Re: Brunswick Hotel & Tavern – Notice of Data Security Incident

Dear «firstname» «lastname»:

Olympia Hotel Management, manager of the Brunswick Hotel & Tavern located at 4 Noble Street, Brunswick, Maine, recently discovered malware on the hotel's computer systems that may have resulted in unauthorized access to name and payment card information. As a recent guest of the hotel, we are writing to provide you with information about this incident, to share the steps that we are taking in response, and to provide you with important information about the steps you can take to reduce the risk of unauthorized use of your personal information. We regret any inconvenience this incident may have caused.

What happened:

Based on our investigation to date, it appears that one of the front desk computers at the hotel was infected with sophisticated malware designed to capture and permit remote access to name and payment card information while avoiding detection by anti-virus software. On August 12, 2015, our security consultants determined that the malware may have been active on that front desk system between November 29, 2014 and July 21, 2015. As a result, your information may have been exposed. Although we do not have conclusive evidence that your information was actually accessed remotely, we have not been able to rule that out and encourage you to take advantage of the credit monitoring and other resources we provide below.

What we are doing to protect your information:

Since the incident was identified, we have taken steps to eliminate the threat posed by the malware and further secure our systems against this type of intrusion. We have retained a leading cybersecurity and investigations company to help us further evaluate the situation and take appropriate action. We have also notified and are working with the major card companies to limit the risk to our guests of fraudulent card charges.

In addition, to help protect your identity, we are offering a complimentary one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. To activate this product please follow the steps below. No credit card is needed for enrollment.

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: November 30, 2015** (Your code will not work after this date.)

2. Visit the **ProtectMyID Web Site to enroll:** http://www.protectmyid.com/alert
3. PROVIDE **Your Activation Code: «Code»**

If you have questions or need an alternative to enrolling online, please call (877) 297-7780 and provide engagement #: **PC96132. For additional details regarding the 12-month ProtectMyID Membership please see the next page of this letter.**

Additional steps you can take to protect your information:

Please remain vigilant to fraud or identity theft, including by reviewing account statements and monitoring credit reports. Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-297-7780.

You may also wish to consult the U.S. Federal Trade Commission on the web at www.consumer.gov/idtheft, by phone at 1-877-438-4338, or by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state's «Regulator» may also have advice on preventing identity theft. You should report instances of known or suspected identity theft to law enforcement, your State's «Regulator» and the FTC. The «Reg_State_Ab» «Regulator» can be contacted at «Reg_Street», «Reg_City», «stateprov» «Reg_Zip»; by telephone at «Reg_Phone»; or on the web at «Reg_Web».

Finally, there are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s), including contacting the three credit reporting agencies at the contact numbers listed on the final page of this letter. Please refer to the final page of this letter for further information.

Please be assured that we are committed to protecting the privacy and security of the sensitive information we collect and have taken and continue to take appropriate steps to respond to this intrusion. Note that neither Olympia Hotel Management nor the Brunswick Hotel & Tavern will contact you to confirm any personal information, nor will any company acting on their behalf. If you are contacted by anyone purporting to represent Olympia or the Brunswick Hotel and asking for your personal information, do not provide it.

If you have any questions or need additional assistance that we can provide, please call our toll-free number at 877-271-1388 (in the U.S.) or 503-520-4424 (outside the U.S.).

Sincerely,

Daniel J. Flaherty
Olympia Hotel Management
Manager of the Brunswick Hotel & Tavern

{W5052120.10}

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian credit report.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance:*** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Please note that these services are offered to the specific addressee of this letter and are not available to anyone other than the individual who received this notification.

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➢ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An **initial 90 day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should takes steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

➢ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

➢ **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit www.annualcreditreport.com or call 877-322-8228.

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➢ **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

➢ **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➢ **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.