haynesboone

July 8, 2016

VIA EMAIL
SecurityBreach@atg.wa.gov

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

Dear Sir or Madam:

Pursuant to Wash. Rev. Code § 19.255.010, I write to notify you of a breach of payment card security at Omni Hotels and Resorts.

On May 30, 2016, Omni discovered it was the victim of malware attacks on its network affecting specific point of sale systems on-site at some Omni properties. The malware was designed to collect certain payment card information, including cardholder name, credit/debit card number, security code and expiration date.

There is no evidence that other customer information, such as contact information, Social Security numbers or PINs, were affected by this issue. The attacks did not affect all of Omni's hotels or systems, and depending on the location, the malware may have operated between December 23, 2015 and June 14, 2016, although most of the systems were affected during a shorter timeframe.

Omni is aware of 316 Washington residents that were potentially affected and has notified consumer reporting agencies. Because the affected systems often did not include addresses or contact information, we are unable to determine the total number of affected Washington residents. Attached for your reference is a copy of the notices Omni will send to affected individuals. Omni is providing written notice (when contact information is available), providing electronic notice (if e-mail addresses are available), providing media notification, and posting a notice to its website. All notices will be provided to individuals on July 8, 2016.

Upon learning of the intrusion, Omni promptly engaged leading IT investigation and security firms approved by the major credit card companies to determine the facts and contain the intrusion. The issue has been resolved, and Omni has taken steps to further strengthen its systems. Omni has contacted law enforcement and is cooperating with its investigation. Out of an abundance of caution, Omni also is offering one year of free identity theft protection and repair to all affected individuals to provide an additional safeguard.

If you have any questions, please contact me using the information below.

Haynes and Boone, LLP
Attorneys and Counselors
2323 Victory Avenue, Suite 700
Dallas, Texas 75219-7672
Phone: 214.651.5000
Fax: 214.651.5940

haynesboone

Sincerely,

Timothy A. Newman
Haynes and Boone, LLP
timothy.newman@haynesboone.com
Direct Dial 214-651-5029

Enclosure

OMNI HOTELS & RESORTS

Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

July 8, 2016

Notice of Data Breach

Dear John Sample:

Omni values the relationship we have with our guests and wants you to be aware of an incident that may involve your payment card. We recently became aware of a malware intrusion that affected some point of sale systems at certain Omni hotels. Promptly after discovering the issue, we immediately engaged leading IT investigation and security firms to determine the facts, and we have now contained the intrusion. Protecting the security of our customers' personal information is a top priority for Omni. We value and respect the privacy of your information, and we sincerely apologize for any concern or inconvenience this may cause you.

1. What Happened and What Information Was Involved:

On May 30, 2016, we discovered we were the victim of malware attacks on our network affecting specific point of sale systems on-site at some Omni properties. The malware was designed to collect certain payment card information, including cardholder name, credit/debit card number, security code and expiration date.

We have no indication that reservation or Select Guest membership systems were affected. Accordingly, if you did not physically present your payment card at a point of sale system at one of the affected Omni locations, we do not believe your payment card was affected. Additionally, there is no evidence that other customer information, such as contact information, Social Security numbers or PINs, were affected by this issue. The attacks did not affect all of our hotels, and depending on the location, the malware may have operated between December 23, 2015 and June 14, 2016, although most of the systems were affected during a shorter timeframe.

2. What We Are Doing and What You Can Do:

Upon learning of the intrusion, we promptly engaged leading IT investigation and security firms approved by the major credit card companies to determine the facts and contain the intrusion. The issue has been resolved, and we have taken steps to further strengthen our systems. We have contacted law enforcement and are cooperating with its investigation.

Even if you used your payment card at one of the properties involved, it does not mean you will be affected by this issue. Out of an abundance of caution, you may want to review and monitor your payment card statements if you used a payment card at an Omni hotel during the above referenced dates. If you believe your payment card may have been affected, please contact your bank or card issuer immediately. We also are offering twelve (12) months of free identity theft protection and repair to all affected guests to provide an added safeguard. Additional information about those services and other steps you can take to protect yourself is available in the attached Reference Guide.

01-02-1-00

3. For More Information:

We sincerely apologize for any inconvenience or concern this incident may cause you. Our guests are our highest priority, and the privacy and protection of our guests' information is a matter we take very seriously. If you have any further questions, please call 1-855-303-9809, Monday through Saturday, 8:00 am to 8:00 pm CST or go to omnihotels.allclearid.com.

Sincerely,

Omni Hotels Management

Reference Guide

It is recommended by some state laws that you remain vigilant, review your relevant account statements, and monitor your credit reports for suspicious activity. Some state laws advise you to report any suspected identity theft to law enforcement, your state's Attorney General, and the Federal Trade Commission. 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, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report:

Equifax
P.O. Box 740241
Atlanta, GA 30348
800-685-1111
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
800-888-4213
www.transunion.com

Fraud Alerts: 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 can be done by contacting the credit bureaus by phone and also via Experian's or Equifax's website. Once you place a fraud alert at one credit bureau, that bureau is required to notify the other two and have alerts placed on your behalf. Note, however, that because the alert tells creditors to follow certain procedures to protect you, it may also delay your efforts to obtain credit while the agency verifies your identity.

Security Freezes: You have the right to place a security freeze on your credit report. A security freeze is intended to prohibit a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please 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.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail. In order to request a security freeze you will need to provide the following information: (1) full name (including middle initial and any suffixes); (2) social security number; (3) date of birth; (4) current address and previous addresses for the past five years; (5) proof of current address, such as a current utility bill, bank statement, or insurance statement; (6) a legible photocopy of a government issued identification card (state driver's license, military identification, etc.); (7) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

Identity Protection: As an added precaution, we have arranged to have AllClear ID protect your identity for twelve (12) months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next twelve (12) months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-303-9809 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Identity Theft Monitoring: This service offers additional layers of protection including identity theft monitoring that delivers secure, actionable alerts to you by phone and $1 million identity theft insurance coverage. To use this service, you will need to provide your personal information to AllClear ID. You may

sign up online at enroll.allclearid.com or by phone by calling 1-855-303-9809 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

Additional Information: If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Residents of Massachusetts and Rhode Island also have the right to obtain any police report filed in regard to this incident. You can further educate yourself regarding fraud alerts, security freezes, and steps you can take toward preventing identity theft by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission can be reached at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/bcp/edu/microsites/idtheft/
1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261

Residents of North Carolina, Rhode Island, and Maryland can obtain information from the North Carolina, Rhode Island, and Maryland Offices of the Attorneys General and the Federal Trade Commission about identity theft and steps they can take toward preventing identity theft.

Maryland Office of the
Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Office of the
Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Rhode Island Office of the
Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400
http://www.riag.ri.gov