Notice of Data Breach (8/12/2016)

HEI Hotels & Resorts ("HEI") recently became aware of a security incident possibly affecting the personal information of some customers who made payment card purchases at point-of-sale terminals, such as food and beverage outlets, at certain HEI managed properties. As a precaution, we are providing this notice, on behalf of our hotel property owners, to make potentially affected customers aware of the incident and call their attention to steps they can take to help protect themselves. We take the security of personal information very seriously, and sincerely apologize for any inconvenience or concern this incident may cause.

What Happened

HEI was recently alerted to a potential security incident by its card processor. Based upon an extensive forensic investigation, it appears that unauthorized individuals installed malicious software on our payment processing systems at certain properties designed to capture payment card information as it was routed through these systems.

What Information Was Involved

We believe the malware could have affected payment card data—including name, payment card account number, card expiration date, and verification code—of customers who used a payment card at point-of-sale terminals at the affected properties and during the period of time identified below:

PROPERTY	ADDRESS	DATES AFFECTED
Boca Raton Marriott at Boca Center	5150 Town Center Cir., Boca Raton, FL 33486	3/1/2015 – 6/7/2015 and 12/15/2015 – 4/11/2016
Dallas Fort Worth Marriott Hotel & Golf Club	3300 Championship Pkwy., Fort Worth, TX 76177	12/26/2015 – 4/28/2016
Equinox Resort Golf Resort & Spa	3567 Main St., Manchester Village, VT 05254	12/23/2015 – 5/4/2016
Hotel Chicago Downtown	333 N. Dearborn St., Chicago, IL 60654	12/26/2015 – 4/27/2016
Hyatt Centric Santa Barbara	1111 E. Cabrillo Blvd., Santa Barbara, CA 93103	12/26/2016 – 6/21/2016
Intercontinental Tampa Bay	4860 W. Kennedy Blvd., Tampa, FL 33609	3/21/2016 – 6/15/2016
Le Meridien Arlington	1121 19th St. N., Arlington, VA 22209	12/23/2015 – 4/28/2016
Le Meridien San Francisco	333 Battery St., San Francisco, CA 94111	3/1/2015 – 6/7/2015 and 12/2/2015 – 6/8/2016
Renaissance San Diego Downtown Hotel	421 W. B St., San Diego, CA 92101	12/26/2015 – 5/2/2016
Royal Palm South Beach Miami	1545 Collins Ave., Miami Beach, FL 33139	12/23/2015 – 6/6/2016
San Diego Marriott La Jolla	4240 La Jolla Village Dr., La Jolla, CA 92037	12/26/2015 – 5/2/2016
Sheraton Music City Hotel	777 McGavock Pike, Nashville, TN 37214	3/1/2015 – 6/8/2016
Sheraton Pentagon City	900 S. Orme St., Arlington, VA 22204	3/3/2015 – 6/7/2015 and 12/2/2015 – 6/13/2016
The Hotel Minneapolis Autograph Collection	215 4th St. South, Minneapolis, MN 55401	3/1/2015 – 4/27/2016
The Westin Minneapolis	88 South 6th St., Minneapolis, MN 55402	9/2/2015 – 6/17/2016
The Westin Pasadena	191 N. Los Robles Ave., Pasadena, CA 91101	3/3/2015 – 5/18/2016
The Westin Philadelphia	99 S. 17th St., Philadelphia, PA 19103	3/10/2016 – 6/6/2016
The Westin Snowmass Resort	100 Elbert Lane, Snowmass Village, CO 81615	12/26/2015 – 4/10/2016
The Westin Washington, D.C. City Center	1400 M St. NW, Washington, DC 20005	11/15/2015 – 5/28/2016
Westin Fort Lauderdale	400 Corporate Dr., Fort Lauderdale, FL 33334	1/29/2016 – 4/13/2016

What We Are Doing

We are treating this matter as a top priority, and took steps to address and contain this incident promptly after it was discovered, including engaging outside data forensic experts to assist us in investigating and remediating the situation and promptly transitioning payment card processing to a stand-alone system that is completely separated from the rest of our network. In addition, we have disabled the malware and are in the process of reconfiguring various components of our network and payment systems to enhance the security of these systems. We have contacted law enforcement and will continue to cooperate with their investigation. We are also coordinating with the banks and payment card companies. While we are continuing to review and enhance our security measures, the incident has now been contained and customers can safely use payment cards at all HEI properties.

What You Can Do

We want to make potentially affected customers aware of steps they can take to guard against fraud or identify theft. We recommend that customers review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge customers to remain vigilant and continue to monitor statements for unusual activity going forward. If they see anything they do not understand or that looks suspicious, or if they suspect that any fraudulent transactions have taken place, customers should immediately notify the issuer of the credit or debit card. In instances of payment card fraud, it is important to note that federal laws and cardholder policies may limit cardholders' responsibility for fraudulent activity; we therefore recommend reporting any suspicious activity in a timely fashion to the bank that issued the card.

We are also providing information and resources to help customers protect their identities, including an "Information About Identity Theft Protection" reference guide, available here, which describes additional steps customers may take to help protect themselves and recommendations from the Federal Trade Commission regarding identity theft protection.

For More Information

For more information about this incident and ways customers can protect themselves, contact us toll-free at 888-849-1113 between 9:00 a.m. and 9:00 p.m. Eastern time, Monday through Friday. Again, we regret any concern this incident may cause.

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: 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.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company. (By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts: P.O. Box 740256, Atlanta, GA 30374
Credit Freezes: P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 1000
Chester, PA 19016
800-888-4213

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872