HILTON WORLDWIDE

Courtney Barton
Senior Counsel
Global Privacy

Hilton Worldwide
7930 Jones Branch Drive
McLean, VA 22102
703-883-5961

November 24, 2015

VIA EMAIL

Washington Office of the Attorney General
securitybreach@atg.wa.gov

Dear Attorney General Ferguson:

Hilton Worldwide, Inc. ("Hilton") is writing to notify you that the company has identified and taken action to eradicate unauthorized malware that may have resulted in the acquisition of the payment card information of Washington residents. The Hilton portfolio of brands include Hilton Hotels & Resorts, Waldorf Astoria Hotels & Resorts, Conrad Hotels & Resorts, Canopy by Hilton, Curio – A Collection by Hilton, DoubleTree by Hilton, Embassy Suites by Hilton, Hilton Garden Inn, Hampton by Hilton, Homewood Suites by Hilton, Home2 Suites by Hilton and Hilton Grand Vacations.

On February 10, 2015, Hilton became aware of potential malware activity targeting its payment card systems through notice from its managed service provider. Hilton immediately launched an internal investigation, and has further strengthened its systems. Hilton retained a leading third-party security expert (the "Expert") to conduct a forensic investigation of the incident, as well as a payment card industry ("PCI") forensic investigator ("PFI"). Hilton also notified participating payment card companies, certain acquiring banks that it was able to identify, and federal law enforcement.

Based on its investigation to date, the PFI has determined that the intruders used malicious software ("malware") to target payment card data on certain Hilton systems between November 18, 2014 and December 5, 2014. The PFI identified two malware output files containing primary account numbers ("PANs") and certain other payment card data. These files contained approximately 26,347 PANs. A subset of these PANs were found in combination with an individual's name; the majority of the PANs were not linked with an individual's name.

Separately, on July 13, 2015, Hilton's intrusion detection system identified potential malware activity on its IT network unrelated to the activity discovered in February 2015. Consistent with its previous response, Hilton promptly commenced an investigation. Based on the preliminary findings of this investigation, Hilton again retained the same Expert and PFI to conduct separate investigations. Hilton also notified participating payment card companies, certain acquiring banks that it was able to identify, and federal law enforcement.

With respect to the second incident, the PFI investigation to date indicates that malware targeted payment card data on certain Hilton systems between April 21, 2015 and July 27, 2015. The malware used during the second incident is distinct in name and operation from the malware used during the first incident. The investigation has identified several malware output files containing PANs and certain other payment card data for approximately 345,147 individuals. A subset of these PANs were found in combination with an individual's name.

Both investigations are ongoing, and thus, the factual findings set forth above are subject to change.

HILTON WORLDWIDE

Courtney Barton
Senior Counsel
Global Privacy

Hilton Worldwide
7930 Jones Branch Drive
McLean, VA 22102
703-883-5961

Throughout both investigations, Hilton has cooperated and shared information with the participating payment card companies, acquiring banks that it was able to identify, and federal law enforcement. In fact, Hilton has held at least biweekly (and often times weekly) status calls with the participating payment card companies and acquiring banks that it has been able to identify on the status and findings of the PFI investigations since the first week of March.

On November 19, 2015, a payment card company notified Hilton that it had received reports from certain payment card issuing banks that they had identified potential fraudulent activity associated with payment cards used at Hilton properties during the time frame of the second incident. As a result of this new information, and even though the third party investigator has not confirmed credit card exfiltration from our systems at this time, Hilton is providing notice and protections to individuals with personal information *potentially* impacted by *both* incidents. Hilton is taking this conservative approach because it values the trust and protection of our guests and their information.

The malware output files did not contain verifiable contact information for the approximately 370,000 potentially impacted individuals. This, combined with the fact that Hilton does not centrally collect and maintain contact information for Hotel guests based on their payment card information, means that Hilton is unable to locate contact information for these individuals. As a result, Hilton is providing substitute notice via a microsite ("hiltonworldwide.com/guestupdate") available through the Hilton website, notice published in major state media, and notice via email (where an email address is available).

In connection with substitute notice, Hilton is offering all individuals who used their payment card at a hotel within the Hilton portfolio one year of free credit monitoring through AllClear ID, a global leader in risk mitigation and response solutions. In addition, even though we have no indication that this incident creates a risk of identity theft, the substitute notice microsite will include information to enable individuals to protect themselves from identify theft, including contact information for the three national credit reporting agencies and the Federal Trade Commission ("FTC"); information on how to obtain a credit report and how to put in place a fraud alert and a credit freeze; and considerations related to monitoring account statements and credit reports, and reporting suspected incidences of identity theft to local law enforcement, the Attorney General, and/or the FTC. The microsite also informs residents that they have the right to obtain a police report. A copy of the microsite materials is enclosed. We also are providing notice of the incident to national credit reporting agencies Equifax, Experian, and TransUnion.

We assure you that Hilton takes the protection of personal information seriously. Should you have any questions or require additional information, please feel free to contact me at 703-883-5961 or courtney.barton@hilton.com.

Sincerely,

Courtney Barton
Senior Counsel, Global Privacy

Encl.

HILTON
WORLDWIDE

November 24, 2015

Message to Our Valued Customers

On behalf of Hilton Worldwide, we sincerely regret any inconvenience related to our recent announcement that we identified and eradicated unauthorized malware that targeted payment card information in some point-of-sale systems at our hotels. You have my personal assurance that we take this matter very seriously, and we immediately launched an investigation and further strengthened our systems. However, as a precautionary measure, some of you may wish to review payment card statements during certain time periods.

You may want to review and monitor your payment card statements if you used a payment card at a Hilton Worldwide hotel over a seventeen-week period, from November 18 to December 5, 2014 or April 21 to July 27, 2015. If you notice any irregular activity on your cards, please contact your financial institution directly for additional support.

We have worked with third-party forensics experts, law enforcement and payment card companies to conduct a thorough investigation. As a result of this investigation, we have determined that the payment card information may have included cardholder names, payment card numbers, security codes and expiration dates, but no addresses or personal identification numbers (PINs).

Please refer to these Frequently Asked Questions for additional information, and click here (beginning noon CST, Nov. 25, 2015) for complimentary one-year credit monitoring that we are offering. We deeply appreciate your understanding as we work to protect your payment card information.

Sincerely,

Jim Holthouser

Executive Vice President, Global Brands

Press Release [LINK]

Frequently Asked Questions [LINK]

For Immediate Release – 4:30 pm ET

Contact:
Chris Brooks
hiltonmedia@hilton.com
(571) 395-1474

Hilton Worldwide Has Identified and Taken Action to Eradicate Malware

McLean, Va., November 24 - Hilton Worldwide (NYSE: HLT) has identified and taken action to eradicate unauthorized malware that targeted payment card information in some point-of-sale systems. Hilton immediately launched an investigation and has further strengthened its systems.

Hilton Worldwide worked closely with third-party forensics experts, law enforcement and payment card companies on this investigation, and determined that specific payment card information was targeted by this malware. This information includes cardholder names, payment card numbers, security codes and expiration dates, but no addresses or personal identification numbers (PINs).

As a precautionary measure, customers may wish to review and monitor their payment card statements if they used a payment card at a Hilton Worldwide hotel over a seventeen-week period, from November 18 to December 5, 2014 or April 21 to July 27, 2015.

Customers generally are not responsible for fraudulent activity on their payment cards, and should contact their financial institution directly if they notice any irregularities. They can also visit hiltonworldwide.com/guestupdate for more details, including how to receive one year of complimentary credit monitoring.

Hilton Worldwide is strongly committed to protecting customers' payment card information, and we sincerely regret any inconvenience this may have caused customers.

About Hilton Worldwide

Hilton Worldwide (NYSE: HLT) is a leading global hospitality company, spanning the lodging sector from luxury and full-service hotels and resorts to extended-stay suites and focused-service hotels. For 96 years, Hilton Worldwide has been dedicated to continuing its tradition of providing exceptional guest experiences. The company's portfolio of twelve world-class global brands is comprised of more than 4,500 managed, franchised, owned and leased hotels and timeshare properties, with more than 745,000 rooms in 97 countries and territories, including Hilton Hotels & Resorts, Waldorf Astoria Hotels & Resorts, Conrad Hotels & Resorts, Canopy by Hilton, Curio – A Collection by Hilton, DoubleTree by Hilton, Embassy Suites by Hilton, Hilton Garden Inn, Hampton by Hilton, Homewood Suites by Hilton, Home2 Suites by Hilton and Hilton Grand Vacations. The company also manages an award-winning customer loyalty program, Hilton HHonors®. Visit news.hiltonworldwide.com for more information and connect with Hilton Worldwide at www.facebook.com/hiltonworldwide, www.twitter.com/hiltonworldwide, www.youtube.com/hiltonworldwide, www.flickr.com/hiltonworldwide, and www.linkedin.com/company/hilton-worldwide.

###

Frequently Asked Questions

1. **What happened?**
   Hilton Worldwide has identified and taken action to eradicate unauthorized malware that targeted payment card information in some point-of-sale systems. Hilton immediately launched an investigation and has further strengthened its systems.

2. **What caused these incidents?**
   These incidents occurred due to unauthorized malware targeting payment card data on computer systems at certain hotels within the Hilton Worldwide portfolio.

3. **What payment card systems were impacted?**
   Hilton Worldwide has identified and taken action to eradicate unauthorized malware that targeted payment card information in some restaurants, gift shops and other point-of-sale systems.

4. **How were the incidents discovered?**
   Hilton initially identified the unauthorized malware through its information security systems and processes. Hilton Worldwide worked closely with third-party forensics experts, law enforcement and payment card companies on this investigation.

5. **How long did the malicious software run?**
   The evidence indicates that the malware ran between November 18, 2014 and December 5, 2014, and between April 21, 2015 and July 27, 2015.

6. **How many properties are impacted?**
   The unauthorized malware targeted payment card information at Hilton Worldwide hotels. The Hilton portfolio includes Hilton Hotels & Resorts, Waldorf Astoria Hotels & Resorts, Conrad Hotels & Resorts, Canopy by Hilton, Curio – A Collection by Hilton, DoubleTree by Hilton, Embassy Suites by Hilton, Hilton Garden Inn, Hampton by Hilton, Homewood Suites by Hilton, Home2 Suites by Hilton and Hilton Grand Vacations.

7. **How many cards are impacted?**
   While we cannot address the actual number of cards impacted, as a precautionary measure, customers may wish to review and monitor their payment card statements if they used a payment card at a Hilton Worldwide hotel over a seventeen week period, from November 18 to December 5, 2014 or April 21 to July 27, 2015.

8. **What information was targeted? Was my Hilton HHonors information impacted?**
   The information impacted includes cardholder names, payment card numbers, security codes and expiration dates, but no addresses, personal identification numbers (PINs) or Hilton HHonors account information.

9. **Have these incidents been resolved?**
   Hilton Worldwide has taken action to eradicate the unauthorized malware. Hilton immediately launched an investigation and has further strengthened its systems. Hilton Worldwide worked closely with third-party forensics experts, law

enforcement and payment card companies on this investigation, and determined that specific payment card information was targeted by this malware. This information includes cardholder names, payment card numbers, security codes and expiration dates, but no addresses or personal identification numbers (PINs).

10. Is it safe to use a payment card at Hilton Worldwide hotel?

Hilton Worldwide has taken action to eradicate the unauthorized malware. Hilton Worldwide worked closely with third-party forensics experts, law enforcement and payment card companies on this investigation, and determined that specific payment card information was targeted by this malware. This information includes cardholder names, payment card numbers, security codes and expiration dates, but no addresses or personal identification numbers (PINs).

11. If I stay at one of your hotels, will my personal information be safe?

Based on discussions with industry experts, compromised credit card information alone generally is not used to open new lines of credit or steal a person's identity. However, as a precautionary measure, customers may wish to review and monitor their payment card statements if they used a payment card at a Hilton Worldwide hotel over a seventeen-week period, from November 18 to December 5, 2014 or April 21 to July 27, 2015. Hilton immediately launched an investigation and has further strengthened its systems. Hilton Worldwide worked closely with third-party forensics experts, law enforcement and payment card companies on this investigation, and determined that specific payment card information was targeted by this malware. This information includes cardholder names, payment card numbers, security codes and expiration dates, but no addresses or personal identification numbers (PINs).

12. How do I know if my credit card has been compromised?

As a precautionary measure, customers may wish to review and monitor their payment card statements if they used a payment card at a Hilton Worldwide hotel over a seventeen week period, from November 18 to December 5, 2014 or April 21 to July 27, 2015.

13. Is my Hilton HHonors cobranded credit card at risk?

As a precautionary measure, customers may wish to review and monitor their payment card statements if they used a payment card at a Hilton Worldwide hotel over a seventeen week period, from November 18 to December 5, 2014 or April 21 to July 27, 2015.

14. What personal information was compromised?

Hilton Worldwide worked closely with third-party forensics experts, law enforcement and payment card companies on this investigation, and determined that specific payment card information was targeted by this malware. This information includes cardholder names, payment card numbers, security codes and expiration dates, but no addresses or personal identification numbers (PINs).

Based on discussions with industry experts, compromised payment card information alone generally is not used to open new lines of credit or steal a

person's identity. As a precautionary measure, customers may wish to review and monitor their payment card statements if they used a payment card at a Hilton Worldwide hotel over a seventeen week period, from November 18 to December 5, 2014 or April 21 to July 27, 2015.

15. Are you offering credit monitoring services?

Hilton is offering one year of free credit monitoring through AllClear. You may sign up online at hiltonworldwide.allclearid.com or by phone by calling 1-855-270-9191 (U.S. & Canada) and +1 512-201-2188 (outside U.S. & Canada).

16. I am concerned that my credit card will be used for fraudulent charges. What should I do?

There are several steps you can take if you are concerned about fraudulent activity.

Based on discussions with industry experts, compromised payment card information alone generally is not used to open new lines of credit or steal a person's identity. As a precautionary measure, you may wish to regularly monitor your payment card account to see if there is any fraudulent or suspicious activity. You can do this through online, email or text alerts from your bank or financial institution. If there is any unauthorized activity, you may want to consider calling the bank or financial institution that issued the card in order to report the issue.

Additionally, you may consider placing a fraud alert on your credit reports to help mitigate potential issues. To do this, you will need to contact one of the three U.S. credit reporting agencies or AllClear's International Service line.

For U.S. Customers:
Equifax: 1-800-525-6285
Experian: 1-888-397-3742
TransUnion: 1-800-680-7289

For Customers Outside the U.S.:
AllClear: +1 512-201-2188

17. Can someone steal my identity with a stolen credit card number?

Based on discussions with industry experts, compromised credit card information alone generally is not used to open new lines of credit or steal a person's identity. However, it never hurts to check your credit report.

18. Will I be liable for any fraudulent charges on my card?

If you identify any irregular activity on your card, you many want to consider contacting the bank or financial institution that issued the card in order to report the issue directly. Your bank or financial institution will be able to provide information about their policy with respect to fraudulent charges.

19. Should I check my credit report?

Based on discussions with industry experts, compromised payment card information alone generally is not used to open new lines of credit or steal a person's identity. However, it is always a good idea to check your credit report regularly.

Hilton is offering one year of free credit monitoring through AllClear. You may sign up online at hiltonworldwide.allclearid.com or by phone by calling 1-855-270-9191 (U.S. & Canada) and +1 512-201-2188 (outside U.S. & Canada).

20. Do I have to pay for the credit report?

You can order a credit report for free from all three credit bureaus once a year. You can do this online at www.annualcreditreport.com, or by phone at 1-877-322-8228.

21. Should I place a fraud alert on my credit report? How can I do that?

Based on discussions with industry experts, compromised payment card information alone generally is not used to open new lines of credit or steal a person's identity. However, you may wish to place a fraud alert on your credit report. This fraud alert statement informs creditors to possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, call any one of the three credit bureaus at the numbers provided below and follow the "Fraud Victim" instructions. The one you call will notify the others to place the alert. When you call the credit bureau fraud line, you will be asked for identifying information and will be given the opportunity to enter a phone number for creditors to call. You may want to make this your cell phone number for convenience in responding to such calls.

For U.S. Customers:
Equifax: 1-800-525-6285
Experian: 1-888-397-3742
TransUnion: 1-800-680-7289

For Customers Outside the U.S.:
AllClear: +1 512-201-2188

22. What should I do if I am concerned about identity theft?

Based on discussions with industry experts, compromised payment card information alone generally is not used to open new lines of credit or steal a person's identity. However, it is always a good idea to regularly review statements from your accounts if you are concerned about identity theft 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 below.

It is a good idea to regularly review your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). Based on discussions with industry experts, compromised credit card information alone, generally is not used to open new lines of credit or steal a person's identity. However, you may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protecting against identity theft:

Federal Trade Commission,
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
http://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
http://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
http://www.ncdoj.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 below.

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 is normally 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 normally also includes 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. It is recommended that each copy be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

Major Credit Reporting Agencies:

For US Customers:
Equifax (www.equifax.com)
P.O. Box 105851
Atlanta, GA 30348 800-685-1111
Equifax Fraud Alerts:
P.O. Box 105069
Atlanta, GA 30348
Equifax Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013

888-397-3742
Experian Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com) P.O. Box 105281
Atlanta, GA 30348
877-322-8228
TransUnion Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872

For Customers Outside the U.S.:
AllClear: +1 512-201-2188

23. Where can I find more information?
Please continue to check this website for updates.