BakerHostetler

Baker&Hostetler LLP

45 Rockefeller Plaza
New York, NY 10111

T 212.589.4200
F 212.589.4201
www.bakerlaw.com

Theodore J. Kobus III
direct dial: 212-271-1504
tkobus@bakerlaw.com

January 14, 2016

VIA OVERNIGHT DELIVERY

Office of the Attorney General
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut St.
Des Moines, IA 50319

Re: Incident Notification

Dear Sir or Madam:

Our client, Hyatt Hotels Corporation ("Hyatt"), recognizes the importance of protecting its customers' payment card data. On November 30, 2015, Hyatt was able to determine capabilities of malware that had been initially detected six days earlier (just prior to Thanksgiving). The malware was designed to target payment card data. Hyatt immediately expanded its investigation and hired leading third-party security experts to examine its payment card network.

On December 23, 2015, Hyatt issued a preliminary statement concerning its then-ongoing investigation into the malware activity by posting a notice on its website and issuing a press release. Findings from the now-complete investigation indicate the potential for unauthorized access to payment card data from cards used onsite at certain Hyatt-managed locations, primarily at restaurants, between August 13, 2015 and December 8, 2015. A small percentage of the at-risk cards were used at spas, golf shops, parking, and a limited number of front desks, or provided to a sales office during this time period. The at-risk window for a limited number of locations began on or shortly after July 30, 2015. The list of affected locations and potential at-risk timeframes has been posted on Hyatt.com.

The malware was designed to search for payment card track data – cardholder name, card number, expiration date and internal verification code – as the data was being routed through affected payment processing systems and then write the data to an output file. The output files predominantly contained track 2 data (which does not contain the cardholder name), but a small percentage contained

track 1 data as well. Although output files were created, we believe that not all of the output files were collected.

Hyatt has identified one Iowa resident where track 1 data from their card was found in an output file and for whom Hyatt also has a physical address or email address, and thus, Hyatt is voluntarily providing this notice to the Office of the Attorney General. Beginning January 19, 2016, a letter will be sent to this individual in accordance with Iowa Code Ann. § 715C.2(1) in substantially the same form as the document enclosed herewith. In addition, because other Iowa residents may be affected, pursuant to IOWA CODE ANN. § 715C.2(1) and commencing January 14, 2016, Hyatt is providing substitute notification to Iowa residents by posting a statement on its website and issuing a press release in substantially the same form as the documents enclosed herewith. Notice is being provided without unreasonable delay.

Hyatt has taken prompt action to resolve this issue and strengthen the security of its systems in order to help prevent this from happening in the future. Hyatt has also been coordinating its efforts with law enforcement and the payment card networks.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Theodore J. Kobus III

Enclosures

cc: David Blasi, Esq.

TO BE DISTRIBUTED ON JANUARY 14 AT 1 PM CENTRAL TIME

HYATT COMPLETES PAYMENT CARD INCIDENT INVESTIGATION

Affected locations and respective at-risk dates are available at www.hyatt.com/protectingourcustomers

CHICAGO (January 14, 2016) – Hyatt Hotels Corporation (NYSE: H) has completed its investigation of the previously announced payment card incident. The investigation identified signs of unauthorized access to payment card data from cards used onsite at certain Hyatt-managed locations, primarily at restaurants, between August 13, 2015 and December 8, 2015. A small percentage of the at-risk cards were used at spas, golf shops, parking, and a limited number of front desks, or provided to a sales office during this time period. The at-risk window for a limited number of locations began on or shortly after July 30, 2015.

The malware was designed to collect payment card data – cardholder name, card number, expiration date and internal verification code – from cards used onsite as the data was being routed through affected payment processing systems. There is no indication that other customer information was affected.

The list of affected locations and respective at-risk dates is available at www.hyatt.com/protectingourcustomers. Hyatt worked quickly with leading third-party cyber security experts to resolve the issue and strengthen the security of its systems. The company also notified law enforcement and the payment card networks. As previously communicated, customers can confidently use payment cards at Hyatt hotels worldwide.

"Protecting customer information is critically important to Hyatt, and we take the security of customer data very seriously," said Chuck Floyd, global president of operations for Hyatt. "We have been working tirelessly to complete our investigation, and we now have more complete information that we want to share so that customers can take steps to protect themselves. Additionally, we want to assure customers that we took steps to strengthen the security of our systems in order to help prevent this from happening in the future."

Hyatt encourages customers to review their payment card account statements closely and to report any unauthorized charges to their card issuer immediately. Customers with questions can visit www.hyatt.com/protectingourcustomers or call 1-877-218-3036 (U.S. and Canada) and +1-814-201-3665 (International) from 7 a.m. to 9 p.m. EST.

The term "Hyatt" is used in this release for convenience to refer to Hyatt Hotels Corporation and/or one or more of its affiliates.

About Hyatt Hotels Corporation

Hyatt Hotels Corporation, headquartered in Chicago, is a leading global hospitality company with a proud heritage of making guests feel more than welcome. Thousands of members of the Hyatt family strive to make a difference in the lives of the guests they encounter every day by providing authentic hospitality. The Company's subsidiaries develop, own, operate, manage, franchise, license or provide services to hotels, resorts, branded residences and vacation ownership properties, including under the ***Hyatt®, Park Hyatt®, Andaz®, Grand Hyatt®, Hyatt Centric™, Hyatt Regency®, Hyatt Place®, Hyatt House®, Hyatt Zilara™, Hyatt Ziva™, Hyatt Residences®*** and ***Hyatt Residence Club®*** brand names and have locations on six continents. As of September 30, 2015, the Company's worldwide portfolio consisted of 627 properties in 52 countries. For more information, please visit ***www.hyatt.com***.

MESSAGE FROM GLOBAL PRESIDENT OF OPERATIONS

Hyatt completes payment card incident investigation

Dear Hyatt Guest,

Protecting customer information is critically important to Hyatt. We have been working tirelessly to complete our previously announced investigation regarding malware that targeted payment card data used at Hyatt-managed locations. We now have more complete information we want to share so that you can take steps to protect yourself.

The investigation identified signs of unauthorized access to payment card data from cards used onsite at certain Hyatt-managed locations, primarily at restaurants, between August 13, 2015 and December 8, 2015. A small percentage of the at-risk cards were used at spas, golf shops, parking, and a limited number of front desks, or provided to a sales office during this time period. The at-risk window for a limited number of locations began on or shortly after July 30, 2015.

The malware was designed to collect payment card data – cardholder name, card number, expiration date and internal verification code – from cards used onsite as the data was being routed through affected payment processing systems. There is no indication that other customer information was affected.

The list of affected Hyatt locations and respective at-risk dates is available here. Additionally, for at-risk transactions where a cardholder's name was affected, we are in the process of mailing letters to customers for whom we have a mailing address and sending emails to customers for whom we only have an email address.

We worked quickly with leading third-party cyber security experts to resolve the issue and strengthen the security of our systems in order to help prevent this from happening in the future. We also notified law enforcement and the payment card networks. Please be assured that you can confidently use payment cards at Hyatt hotels worldwide.

Most importantly, we encourage you to remain vigilant and to review your payment card account statements closely. You should report any unauthorized charges to your card issuer immediately. Speak to your card issuer for details because, while card issuers' policies related to fraud may vary, payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner.

Additionally, Hyatt has arranged for CSID to provide one year of CSID's Protector services to affected customers at no cost to them. CSID is one of the leading providers of fraud detection solutions and technologies. In order to activate CSID's Protector coverage, affected customers in the U.S. may visit www.csid.com/hyatt-us and affected customers outside the U.S. may visit www.csid.com/hyatt-intl to complete a secure sign up and enrollment process. You should also review the additional information in the Reference Guide on ways to protect yourself.

If you have questions or would like more information, please call 1-877-218-3036 (U.S. and Canada) or +1-814-201-3665 (International) from 7 a.m. to 9 p.m. EST.

Please be assured that we take the security of customer data very seriously. We deeply regret the inconvenience and any concern this may have caused you.

Sincerely,

Chuck Floyd
Global President of Operations
Hyatt Hotels Corporation

Frequently Asked Questions
Hotel List
Reference Guide
Press Release

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740256, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com,1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022-2000, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW
Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

If you are a resident of Maryland, you may contact the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

If you are a resident of Massachusetts, note that pursuant to Massachusetts law, you have the right to obtain a copy of any police report.

Massachusetts law also allows consumers to request a security freeze. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. 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.

The fee for placing a security freeze on a credit report is $5.00. If you are a victim of identity theft and submit a valid investigative report or complaint with a law enforcement agency, the fee will be waived. In all other instances, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. If you have not been a victim of identity theft, you will need to include payment to the credit reporting agency to place, lift, or remove a security freeze by check, money order, or credit card.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

Equifax, PO Box 740256, Atlanta, GA 30374,www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com,1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022-2000,www.transunion.com, 1-800-680-7289

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

If you are a resident of North Carolina, you may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400.

If you are a resident of West Virginia, you also have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is as follows:

Equifax, PO Box 740256, Atlanta, GA 30374,www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com,1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022-2000,www.transunion.com, 1-800-680-7289

As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional

information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft/.

You may also obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a security freeze on your credit report pursuant to West Virginia law. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique personal identification number ("PIN") or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

(1) The unique personal identification number ("PIN") or password provided by the consumer reporting agency;
(2) Proper identification to verify your identity; and
(3) The period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request.

A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit.

[Hyatt letterhead]

January 19, 2016

[first name][last name]
[address]
[city][state][zip]

Dear [first name][last name]:

Protecting customer information is critically important to Hyatt. We have been working tirelessly to complete our previously announced investigation regarding malware that targeted payment card data used at Hyatt-managed locations. We now have more complete information we want to share so that you can take steps to protect yourself.

The investigation identified signs of unauthorized access to payment card data from cards used onsite at certain Hyatt-managed locations, primarily at restaurants, between August 13, 2015 and December 8, 2015. A small percentage of the at-risk cards were used at spas, golf shops, parking, and a limited number of front desks, or provided to a sales office during this time period. The at-risk window for a limited number of locations began on or shortly after July 30, 2015.

The malware was designed to collect payment card data – cardholder name, card number, expiration date and internal verification code – from cards used onsite as the data was being routed through affected payment processing systems. There is no indication that other customer information was affected. The list of affected Hyatt locations and respective at-risk dates is available at www.hyatt.com/protectingourcustomers.

We worked quickly with leading third-party cyber security experts to resolve the issue and strengthen the security of our systems in order to help prevent this from happening in the future. We also notified law enforcement and the payment card networks. Please be assured that you can confidently use payment cards at Hyatt hotels worldwide.

Most importantly, we encourage you to remain vigilant and to review your payment card account statements closely. You should report any unauthorized charges to your card issuer immediately. Speak to your card issuer for details because, while card issuers' policies related to fraud may vary, payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner.

Additionally, Hyatt has arranged for CSID to provide one year of CSID's Protector services at no cost to you. CSID is one of the leading providers of fraud detection solutions and technologies. In order to activate CSID's Protector coverage, please visit www.csid.com/hyatt-us to complete a secure sign up and enrollment process. You should also review the additional information on ways to protect yourself enclosed with this letter.

If you have questions or would like more information, please call 1-877-218-3036 from 7 a.m. to 9 p.m. EST.

Please be assured that we take the security of customer our data very seriously. We deeply regret the inconvenience and any concern this may have caused you.

Sincerely,

Chuck Floyd
Global President of Operations
Hyatt Hotels Corporation

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740256, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com,1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022-2000, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW
Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.