BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

April 14, 2017

VIA EMAIL (SECURITYBREACH@ATG.WA.GOV)
AND OVERNIGHT MAIL

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Attorney General Ferguson:

Our client is Six Continents Hotels, Inc. which is an InterContinental Hotels Group Company ("IHG"). Most IHG-branded locations are independently owned and operated by separate entities that have a franchise license from IHG. IHG is submitting this notification on behalf of certain franchisees that operated locations in the Americas. After several franchisees were made aware in January 2017 by payment card networks of patterns of unauthorized charges occurring on payment cards after they were legitimately used at their locations and reported those notices to IHG, to ensure an efficient and effective response, IHG hired a leading cyber security firm on behalf of franchisees to coordinate an examination of the payment card processing systems of franchise hotel locations in the Americas region.

The investigation identified signs of the operation of malware designed to access payment card data from cards used onsite at the front desk at certain IHG-branded franchise hotel locations in the Americas between September 29, 2016 and December 29, 2016. The malware searched for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the affected hotel server. There is no indication that other guest information was affected. Before this incident began, many IHG-branded franchise hotel locations had implemented IHG's Secure Payment Solution (SPS), a point-to-point encryption payment acceptance solution. Properties that had implemented SPS before September 29, 2016, were not affected. Many more properties implemented SPS after

September 29, 2016, and the implementation of SPS ended the ability of the malware to find payment card data and, therefore, cards used at these locations after SPS implementation were not affected.

On behalf of franchisees, beginning today, IHG is mailing a notification letter to 13,825 Washington residents in accordance with Wash. Rev. Code § 19.255.010 in substantially the same form as the letter attached hereto. Also, pursuant to Wash. Rev. Code § 19.255.010(8)(c), on behalf of franchisees, IHG is providing substitute notification today by posting a statement on its website (www.ihg.com/protectingourguests) and links to the statement on the homepages of Intercontinental.com, Hotelindigo.com, Crowneplaza.com, Holidayinnresorts.com, Holidayinn.com, Staybridge.com, and Candlewoodsuites.com and issuing a press release (a copy of the press release and substitute notice are enclosed). Notice is being provided as expeditiously as practicable and without delay.

IHG has established a dedicated call center that potentially affected individuals can contact with questions. IHG is also recommending that potentially affected individuals remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity.

On behalf of franchisees, IHG has been working closely with the payment card networks as well as with the cyber security firm to confirm that the malware has been eradicated and evaluate ways for franchisees to enhance security measures. Law enforcement has also been notified.

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

Sincerely,

Craig A. Hoffman

Enclosures

IHG®

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

IHG values the relationship we have with our guests and understands the importance of protecting payment card data. Regrettably, on behalf of our franchisees, we are writing to inform you of an incident involving some of that information.

Many IHG-branded locations are independently owned and operated franchises, and certain of these franchisee operated locations in the Americas were made aware by payment card networks of patterns of unauthorized charges occurring on payment cards after they were legitimately used at their locations. To ensure an efficient and effective response, IHG hired a leading cyber security firm on behalf of franchisees to coordinate an examination of the payment card processing systems of franchise hotel locations in the Americas region.

The investigation identified signs of the operation of malware designed to access payment card data from cards used onsite at the front desk at certain IHG-branded franchise hotel locations in the Americas* between September 29, 2016 and December 29, 2016. The malware searched for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the affected hotel server. There is no indication that other guest information was affected. You are being notified because you used payment card(s) ending in <<ClientDef1(Card Number)>> during this time period onsite at the front desk of an affected hotel. A list of affected IHG franchise locations and respective time frames, which may vary by location, is available at *www.ihg.com/protectingourguests*.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take.

On behalf of franchisees, IHG has been working closely with the payment card networks as well as with the cyber security firm to confirm that the malware has been eradicated and evaluate ways for franchisees to enhance security measures. Law enforcement has also been notified.

We deeply regret any inconvenience this may have caused. If you have questions, please call 855-330-6367 from 8:00 a.m. to 8:00 p.m. ET, Monday to Friday.

Sincerely,

Elie Maalouf
Chief Executive Officer, The Americas
IHG

* *The affected IHG hotel brands in the Americas are Hotel Indigo®, Crowne Plaza® Hotels & Resorts, Holiday Inn® Hotels & Resorts, Holiday Inn Express®, Staybridge Suites® and Candlewood Suites®.*

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free 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 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, 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. 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. 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

InterContinental Hotels Group (IHG) Notifies Guests of Payment Card Incident at IHG-Branded Franchise Hotel Locations in the Americas Region

April 14, 2017

California residents please click here

IHG values the relationship we have with our guests and understands the importance of protecting payment card data. Many IHG-branded locations are independently owned and operated franchises, and certain of these franchisee operated locations in the Americas were made aware by payment card networks of patterns of unauthorized charges occurring on payment cards after they were legitimately used at their locations. To ensure an efficient and effective response, IHG hired a leading cyber security firm on behalf of franchisees to coordinate an examination of the payment card processing systems of franchise hotel locations in the Americas region.

The investigation identified signs of the operation of malware designed to access payment card data from cards used onsite at front desks for certain IHG-branded franchise hotel locations between September 29, 2016 and December 29, 2016. Although there is no evidence of unauthorized access to payment card data after December 29, 2016, confirmation that the malware was eradicated did not occur until the properties were investigated in February and March 2017. Before this incident began, many IHG-branded franchise hotel locations had implemented IHG's Secure Payment Solution (SPS), a point-to-point encryption payment acceptance solution. Properties that had implemented SPS before September 29, 2016 were not affected. Many more properties implemented SPS after September 29, 2016, and the implementation of SPS ended the ability of the malware to find payment card data and, therefore, cards used at these locations after SPS implementation were not affected.

The malware searched for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the affected hotel server. There is no indication that other guest information was affected. A list of affected IHG franchise locations and respective time frames, which may vary by location, is available *here*.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take.

On behalf of franchisees, IHG has been working closely with the payment card networks as well as with the cyber security firm to confirm that the malware has been eradicated and evaluate ways for franchisees to enhance security measures. Law enforcement has also been notified.

We regret any inconvenience this may have caused. If you have questions, and reside in the United States, please call 855-330-6367 from 8:00 a.m. to 8:00 p.m. ET, Monday to Friday. If you reside outside the United States, please call 800-290-9989 from 8:00 a.m. to 8:00 p.m. ET, Monday to Friday.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free 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
Phone: 1-800-685-1111
P.O. Box 740256
Atlanta, Georgia 30348
www.equifax.com

Experian
Phone: 888-397-3742
P.O. Box 9554
Allen, Texas 75013
www.experian.com

TransUnion
Phone: 800-916-8800
P.O. Box 2000
Chester, PA 19106
www.transunion.com

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. 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. 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

---

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 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 or toll free at 1-877-566-7226.

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 Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19022-2000, www.transunion.com

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 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, 1-800-685-1111
Experian, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, 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.

For Canadian residents: We recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your financial statements for any unauthorized activity. To obtain a copy of your credit report, you can contact the two Canadian credit reporting companies directly. Your free credit report is called a "credit file disclosure" by Equifax Canada and a "consumer disclosure" by TransUnion Canada. It does not include your credit score. To get your credit report free of charge, you may order it by mail, fax, telephone, or in person. If you choose to access it online, you will have to pay a fee.

- Equifax Canada, Consumer Relations Department, P.O. Box 190, Station Jean-Talon, Montreal, QC H1S 2Z2, 1-800-465-7166, www.equifax.ca

- TransUnion Canada, Consumer Relations Centre, P.O. Box 338, LCD 1, Hamilton, ON L8L 7W2, 1-800-663-9980, www.transunion.ca

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 your local police force and file a report. You should also report identity theft and fraud to the Canadian Anti-Fraud Centre at info@antifraudcentre.ca.

FOR IMMEDIATE RELEASE

InterContinental Hotels Group (IHG) Notifies Guests of Payment Card Incident at IHG-Branded Franchise Hotel Locations in the Americas Region

ATLANTA – [Date of Release] – IHG values the relationship it has with its guests and understands the importance of protecting payment card data. Many IHG-branded locations are independently owned and operated franchises, and certain of these franchisee operated locations in the Americas were made aware by payment card networks of patterns of unauthorized charges occurring on payment cards after they were legitimately used at their locations. To ensure an efficient and effective response, IHG hired a leading cyber security firm on behalf of franchisees to coordinate an examination of the payment card processing systems of franchise hotel locations in the Americas region.

The investigation identified signs of the operation of malware designed to access payment card data from cards used onsite at the front desk at certain IHG-branded franchise hotel locations between September 29, 2016 and December 29, 2016. Although there is no evidence of unauthorized access to payment card data after December 29, 2016, confirmation that the malware was eradicated did not occur until the properties were investigated in February and March 2017. Before this incident began, many IHG-branded franchise hotel locations had implemented IHG's Secure Payment Solution (SPS), a point-to-point encryption payment acceptance solution. Properties that had implemented SPS before September 29, 2016 were not affected. Many more properties implemented SPS after September 29, 2016, and the implementation of SPS ended the ability of the malware to find payment card data and, therefore, cards used at these locations after SPS implementation were not affected.

The malware searched for track data (which sometimes has cardholder name in addition to card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the affected hotel server. There is no indication that other guest information was affected. A list of affected franchise locations and respective time frames, which may vary by location, is available at *www.ihg.com/protectingourguests*. The site also contains more information on steps guests may take.

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card.

On behalf of franchisees, IHG has been working closely with the payment card networks as well as with the cyber security firm to confirm that the malware has been eradicated and evaluate ways for franchisees to enhance security measures. Law enforcement has also been notified. IHG also has established a dedicated call center to answer any questions affected guests may have.

For additional information about this incident, please visit the IHG website at *www.ihg.com/protectingourguests*.

###

Media Contact:
Neil Hirsch
neil.hirsch@ihg.com