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