



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

### **Notice of Data Breach**

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.

#### **What Happened**

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.

#### **What Information Was Involved**

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](http://www.ihg.com/protectingourguests).

#### **What You Can Do**

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.

#### **What We Are Doing**

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.

**For More Information**

We deeply regret any inconvenience this may have caused. If you have questions, please call 855-330-6367 from 5:00 a.m. to 5:00 p.m. PT, 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](http://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](http://www.equifax.com), 1-800-685-1111

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://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](http://www.ftc.gov/idtheft)