

[InterContinental Mark Hopkins - San Francisco Hotel Letterhead]

[Vermont Customer Notification Letter]

[Return Address]

August [], 2013

Return Receipt Requested

[Recipient's Name]

[Address]

[City, State, Zip]

Important Security and Protection Notification.
Please read this entire letter.

Re: Your Credit Card Ending in [XXXX (last 4 digits)]

Dear [Name]:

We are writing to inform you of a potential data security incident that occurred at the InterContinental Mark Hopkins - San Francisco hotel (the "Hotel") on July 4, 2013 that appears to have exposed your payment card account number and other personal information to unauthorized persons.

Please note that we take this incident very seriously and are working closely with the San Francisco Police Department to apprehend the criminals responsible and prosecute them to the fullest extent possible. The Hotel deeply values customer privacy and data protection and regrets this incident. Please be assured that we have taken every step necessary to address this incident and that we remain committed to protecting the information that you have provided to us. At this time, we are unaware of any fraudulent use of your information.

What Happened? On July 4, 2013, two criminals entered the Hotel and ransacked its sales office. They removed a hard drive containing personal data of some of our guests from a computer, and left the hard drive in the sales office. We engaged data security experts to investigate this incident thoroughly and learned on July 14, 2013 that even though the computer hard drive was not taken, it is possible that it was accessed while the criminals were in the office. If the criminals did this, they could have accessed the following types of information: name, mailing address, and credit/debit card number. Fortunately, the information potentially accessed did **NOT** include Social Security Numbers.

What is the Hotel Doing to Protect Me? Please be assured that we have undertaken extensive forensic and other steps to address this incident and that we remain committed to protecting the information that you have provided to us. The Hotel's security department has taken steps to increase security to help prevent such an incident from happening again.

Your payment card company will be provided with your actual card number that may have been accessed during this incident. They may contact you to verify charges in the event that they detect an unusual pattern of charges. If they suspect your account has been compromised, you may receive a new payment card. **We recommend that you also immediately notify your credit card issuing bank** and follow their advice with regard to your payment card.

What are the Risks that My Information Will be Misused? Although we have no reason to believe that there has been any fraudulent use of your information at this time, there is a possibility that your payment card number may be misused. If you notice any fraudulent activity on your payment card, please report it immediately to your financial institution.

What Should I Do? As always, you should remain vigilant and continue to carefully review your payment card account statements and alert your financial institution to any inappropriate charges. This is the most important step that you can take to detect any unauthorized use of your payment card number. If your payment card number is changed, remember to take any necessary steps relating to your bills that are automatically charged to your payment card.

Should I Do Anything Else? Although your Social Security Number was **NOT** exposed, it is generally a good practice to monitor your consumer reports annually. You may obtain a free copy of your credit report once every 12 months from each of the nationwide consumer reporting agencies by visiting <http://www.annualcreditreport.com> or by contacting the consumer reporting agencies listed below:

Equifax

(800) 685-1111
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian

(888) 397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion

(800) 916-8800
P.O. Box 6790
Fullerton, CA 92834
www.transunion.com

We also recommend that you carefully review all your other financial account statements during the next 24 months to make certain there have been no unauthorized transactions made or new accounts opened in your name. Contact your financial institutions immediately if there is any unauthorized activity on your accounts or if an unauthorized account has been opened in your name.

If you want to learn more about how to avoid identity theft, please visit the U.S. government's identity theft information website, <http://www.consumer.gov/idtheft>. You can also contact the Federal Trade Commission via phone at 1-877-ID-THEFT (877-428-4338) or via mail at: Federal Trade Commission - Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Is There Anything Else I Should Know? Please note that we maintain numerous safeguards to protect your personal information, and we have taken steps to prevent any future unauthorized access by bolstering the physical security of our hotel offices. Again, we sincerely regret that this incident occurred and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to call 888-829-6553 to speak to a specially-trained Customer Care Agent.

Sincerely,

Nelum Gunewardane
General Manager