Kimpton Hotels & Restaurants Notifies Customers of Payment Card Incident

August 31, 2016

NOTICE OF DATA BREACH

Kimpton Hotels & Restaurants values the relationship we have with our guests and understands the importance of protecting personal information. We are notifying you of an incident that may involve your payment card information.

What Happened

Kimpton Hotels & Restaurants received a report on July 15, 2016 of unauthorized charges occurring on payment cards after they had been used by guests at the restaurant in one of our hotels. We immediately began to investigate the report and hired leading cyber security firms to examine our payment card processing system. Findings from the investigation show that malware was installed on servers that processed payment cards used at the restaurants and front desks of some of our hotels. The malware searched for track data read from the magnetic stripe of a payment card as it was being routed through the affected server.

This incident involved cards used at certain restaurants and hotel front desks from February 16, 2016 to July 7, 2016. A list of the affected hotel front desks and restaurants, along with the specific time frames for each (times vary by location) is located here. We do not have information available to identify the name and address of restaurant guests. We will be mailing letters to those guests who used their card at a front desk during an at risk time frame for whom we have a mailing address.

What Information Was Involved

The malware primarily found track data that contained the card number, expiration date, and internal verification code, but in a small number of instances it may have found the track that also contains the cardholder name.

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 to protect your information.

What We Are Doing

We have resolved the issue and continue to work with the cyber security firms to further strengthen our existing security measures. We notified law enforcement and are also working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring on the affected cards.

<u>For More Information</u>

We regret any inconvenience this may have caused. If you have questions, please call (888) 339-3142 from 9:00 a.m. to 8:00 p.m. EST, Monday to Friday.

FOR IMMEDIATE RELEASE

Kimpton Hotels & Restaurants Notifies Customers of Payment Card Incident

San Francisco, CA – August 31, 2016 – Kimpton Hotels & Restaurants has completed its investigation of the previously announced payment card security incident.

Kimpton Hotels & Restaurants received a report on July 15, 2016 of unauthorized charges occurring on payment cards after they had been used by guests at the restaurant in one of our hotels. We immediately began to investigate the report and hired leading cyber security firms to examine our payment card processing system. Findings from the investigation show that malware was installed on servers that processed payment cards used at the restaurants and front desks of some of our hotels. The malware searched for track data read from the magnetic stripe of a payment card as it was being routed through the affected server. The malware primarily found track data that contained the card number, expiration date, and internal verification code, but in a small number of instances it may have found the track that also contains the cardholder name.

This incident involved cards used at certain restaurants and and hotel front desks from February 16, 2016 to July 7, 2016. A list of the affected hotel front desks and restaurants, along with the specific time frames for each (times vary by location) is located at www.kimptonhotels.com/protectingourguests. The site also contains more information on steps guests may take to protect their information. Kimpton Hotels & Restaurants does not have information available to identify the name and address of restaurant guests. We will be mailing letters to those guests who used their card at a front desk during an at risk time frame for whom we have a mailing address.

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.

We have resolved the issue and continue to work with the cyber security firms to further strengthen our existing security measures. We notified law enforcement and are also working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring on the affected cards.

We regret any inconvenience this may have caused. If you have questions, please call (888) 339-3142 from 9:00 a.m. to 8:00 p.m. EST, Monday to Friday.

[Kimpton Hotels & Restaurants letterhead]

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

RE: <u>Notice of a Data Breach</u>

Dear [First name] [Last name]:

Kimpton Hotels & Restaurants values the relationship we have with our guests and understands the importance of protecting personal information. We are writing to notify you of an incident that may involve your payment card information.

What Happened

Kimpton Hotels & Restaurants received a report on July 15, 2016 of unauthorized charges occurring on payment cards after they had been used by guests at the restaurant of one of our hotels. We immediately began to investigate the report and hired leading cyber security firms to examine our payment card processing system. Findings from the investigation show that an unauthorized person installed malware on certain servers that processed payment cards used at some of our hotels. The malware searched for track data read from the magnetic stripe of payment cards as it was being routed through the affected servers. We are notifying you because you used your payment card at the front desk of the [affected Kimpton Hotel] between February 16, 2016 and July 7, 2016.

What Information Was Involved

The malware primarily found track data that contained the card number, expiration date, and internal verification code, but in some instances it found the track that also contains the cardholder name.

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.

What We Are Doing

We have resolved the issue and continue to work with the cyber security firms to further strengthen our existing security measures. We notified law enforcement and are also working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring on the affected cards.

For More Information

We regret any inconvenience this may have caused. If you have questions, please call (888) 339-3142 from 9:00 a.m. to 8:00 p.m. EST, Monday to Friday.

Sincerely,

Mike DeFrino
CEO
Kimpton Hotels & Restaurants