LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Sean B. Hoar
888 SW Fifth Avenue, Suite 900
Portland, Oregon 97204-2025
Sean.Hoar@lewisbrisbois.com
Direct: 971.712.2795

July 28, 2017

File No. 28759.911

**VIA E-MAIL (DOJ-CPB@doj.nh.gov)**

Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

I represent Kimpton Hotels & Restaurants ("Kimpton"), located in San Francisco, California. This letter is being sent pursuant to N.H. Rev. Stat. §§359-C:19-21 because on June 6, 2017, Kimpton learned that personal information may have been involved in a data security incident on the Sabre Hospitality Solutions SynXis Central Reservations system ("Sabre"). It has taken time to determine which individuals were affected, and on July 11, 2017, we determined that approximately 88 residents of New Hampshire may have been affected. However, the process to determine the precise number of individuals affected is ongoing. The incident may have involved unauthorized access of payment card information for hotel reservations, including names, card numbers, card expiration dates, and card security codes. In some cases, e-mail addresses, telephone numbers and mailing addresses may have been involved.

On May 2, 2017, Sabre, an independent, third-party provider of reservation services, disclosed that it was investigating the data security incident. As a company that enlists Sabre as a third-party vendor, Kimpton received notification from Sabre on June 6, 2017, that the above-referenced information within Sabre's system may have been accessed without authorization between August 10, 2016 and March 9, 2017. Kimpton confirmed that Sabre investigated the incident with assistance from a digital forensics firm and notified law enforcement and payment card brands in order to prevent fraudulent activity. The data security incident did not occur on, nor did it affect, Kimpton's systems or the systems of its parent company, IHG.

Kimpton is in the process of notifying the affected New Hampshire residents via the attached letter. Kimpton is also providing substitute notice through a link on the Kimpton homepage to a Sabre microsite, http://www.sabreconsumernotice.com/ and a press release. Please contact me should you have any questions.

Very truly yours,

Sean B. Hoar of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Consumer Notification Letter

KIMPTON®
HOTELS & RESTAURANTS

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<Mail ID>
<Name>
<Address1>
<Address2>
<City>, <ST> <ZIP>

<<Date>>

NOTICE OF SABRE PAYMENT CARD INCIDENT

Dear Valued Customer:

You may have recently heard about an incident of unauthorized access of Sabre Hospitality Solutions SynXis Central Reservations system (Sabre), an independent, third-party provider of reservation services, that may have involved your personal information. Sabre facilitates the booking of hotel reservations made by consumers through hotels, online travel agencies, and similar booking services. As one of many companies that enlists Sabre as a third-party vendor and was affected by this incident, we want to make you aware of the steps you can take to protect your personal information.

**What Happened?** On May 2, 2017, Sabre disclosed a data security incident that may have affected personal information. Sabre launched an investigation and engaged a digital forensics firm to assist in this investigation. On June 6, 2017, Kimpton received notification from Sabre that information within Sabre's system was accessed without authorization. Sabre advised that certain reservation information may have been accessed between August 10, 2016 and March 9, 2017. The data security incident did not occur on, nor did it affect, Kimpton's systems nor the systems of its parent company, IHG.

**What Information Was Involved?** Sabre informed Kimpton that the unlawful access may have involved payment card information for hotel reservations, including names, card numbers, card expiration dates, and card security codes. In some cases, email addresses, phone numbers, and mailing addresses may have been involved.

**What We Are Doing:** We confirmed Sabre investigated the incident with assistance from a digital forensics firm and notified law enforcement and the payment card brands in order to prevent fraudulent activity. Kimpton is notifying you of the Sabre incident and providing you information about how you can protect your personal information.

**What You Can Do:** Please review the recommendations on the following page to protect your personal information.

**For More Information:** Sabre has provided a dedicated call center. If you have questions and reside in the United States, please call 800-536-6580, 24 hours a day, Monday to Friday. If you reside outside the United States, please call 503-597-7711, 24 hours a day, Monday to Friday. For additional information about this incident, please visit the Sabre website at www.sabreconsumernotice.com.

Sincerely,

Michael DeFrino
CEO, Kimpton Hotels & Restaurants

## STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**
As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and / or the Federal Trade Commission (FTC).

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

**Equifax**
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

**Experian**
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

**TransUnion**
P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

**Free Annual Report**
P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
annualcreditreport.com

**Fraud Alert:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

**Security Freeze:** In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

**Federal Trade Commission**
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

**Maryland Attorney General**
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

**North Carolina Attorney General**
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

**Rhode Island Attorney General**
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400