WINSTON
&STRAWN
LLP

North America Europe Asia

200 Park Avenue
New York, NY 10166
T +1 212 294 6700
F +1 212 294 4700

Kari M. Rollins
Partner
(212) 294-2664
karollins@winston.com

July 10, 2015

VIA FEDERAL EXPRESS

Attorney General Joseph Foster
Office of the Attorney General
NH Department of Justice
33 Capitol Street
Concord, NH 03301

Re: Notice Concerning Data Incident

Dear Attorney General Foster:

We are writing on behalf of our client, Mandarin Oriental, to report that personal information belonging to Mandarin Oriental guests may have been compromised as the result of a malware attack on the credit card systems at a limited number of Mandarin hotels.

On February 25, 2015, Mandarin Oriental was alerted to the suspected malware attack and immediately launched a forensic investigation into the incident, working in close coordination and cooperation with law enforcement and the credit card companies. From its investigation, Mandarin Oriental believes the hacker may have used a new variant of malware to obtain access to its hotel credit card systems beginning on or around June 18, 2014. Mandarin Oriental believes the hacker may have used this new variant of malware to acquire the credit card numbers and names of individuals who used a credit card to purchase accommodation, spa, dining, or other products and services at the impacted Mandarin Oriental hotel properties.

Based on the investigative results to-date, Mandarin Oriental has confirmed that there are 30 New Hampshire residents whose credit card numbers and names may have been acquired without authorization by the hacker. While the investigation has not shown any evidence that their information was misused, out of an abundance of caution, and in order to provide potentially impacted individuals with information they can use to protect themselves as soon as possible, Mandarin Oriental is sending notice to these individuals on July 10, 2015. Mandarin

Oriental has timed this notice so as not to disrupt or impede the ongoing investigations of law enforcement and the credit card companies. A copy of that notice is attached.

To protect its guests, Mandarin Oriental has taken several steps to remove the malware, ensure the hacker is no longer in its systems, and prevent further unauthorized access of personal information contained in its databases. Additionally, even though Mandarin Oriental has no evidence that credit card information has been improperly used, it is offering free credit monitoring for one year to guests impacted by this incident.

We assure you that our client takes this issue, and the privacy and security of its guests, very seriously and is working diligently to ensure that this does not occur again. Please feel free to contact me if you have any questions.

Best regards,

Kari M. Rollins

Enclosure[s]

MANDARIN ORIENTAL
THE HOTEL GROUP SM

[Date]

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

Dear [first name, last name],

We are writing to advise you that investigations by Mandarin Oriental have regrettably confirmed that the names and credit card numbers of some of our guests appear to have been acquired without authorization. Our investigations have not found, however, any evidence of acquisition or misuse of credit card pin numbers or security codes, or any other personal guest data. We take very seriously the safety and security of our guests and their personal information, and the trust you place in us remains our absolute priority. This incident is the result of a malware attack experienced by a number of Mandarin Oriental hotels listed below. We are contacting you because our records indicate that you may have used a credit card for dining, beverage, spa, guest rooms, or other products and services at one of the affected hotels during the following time periods:

Mandarin Oriental, Boston between June 18, 2014 and March 12, 2015
Mandarin Oriental, Geneva between June 18, 2014 and March 3, 2015
Mandarin Oriental, Hong Kong between June 18, 2014 and February 10, 2015
Mandarin Oriental Hyde Park, London between June 18, 2014 and March 5, 2015
Mandarin Oriental, Las Vegas between June 18, 2014 and October 16, 2014
Mandarin Oriental, Miami between June 18, 2014 and March 3, 2015
Mandarin Oriental, New York between June 18, 2014 and January 18, 2015
Mandarin Oriental, San Francisco between June 18, 2014 and February 14, 2015
Mandarin Oriental, Washington DC between June 18, 2014 and January 20, 2015
The Landmark Mandarin Oriental, Hong Kong between June 18, 2014 and February 3, 2015

We are very sorry for any inconvenience caused by this unfortunate incident.

When we first learned that some of our hotels were the target of a malware attack, we issued a public statement on our website to alert our guests to the attack so they could take proactive measures to monitor their credit card activity. At the same time, we immediately initiated a comprehensive forensic investigation and engaged with law enforcement and the credit card companies. Since then, we have been working in coordination with them, and investigating this incident across multiple countries and properties. We have also taken comprehensive steps to ensure that the malware has been removed and is no longer in our systems.

Although we have no evidence that your personal information has been misused, we treat this matter with the utmost seriousness and want to make sure you have the information you need so that you can take steps to protect yourself. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, your Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps in this letter.

Free Credit Monitoring

To further assist you, we have arranged for you to receive 12 months of free identity protection through Experian's ProtectMyID Alert program. This membership includes identity theft resolution services, a free credit report, daily credit monitoring to detect suspicious activity, and a $1 million identity theft insurance policy, including coverage of unauthorized electronic fund transfers from your bank account. Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis, Inc. The description provided in this letter is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

To offer added protection, you will receive ExtendCARE, which will provide you with fraud resolution support even after your ProtectMyID membership has expired. **Again, this protection is being offered at no cost to you.** You can register for these services by visiting the ProtectMyID Web Site: www.protectmyid.com/alert or calling (877) 297-7780 and providing the following activation code: **[MAILING HOUSE TO INSERT]**. You have until **January 31, 2016** to register. If you have questions or need an alternative to enrolling online, please call (877) 297-7780 and provide Engagement # PC95244. Enrollment in ProtectMyID membership does not affect your credit score.

Placing a Fraud Alert on Your Credit File

You can also place a fraud alert with the major credit reporting agencies on your credit files, their contact information is as follows:

Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069	800-525-6285	www.equifax.com
Experian	Experian Fraud Reporting P.O. Box 9554 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

A fraud alert lasts 90 days, and requires potential creditors to use "reasonable policies and procedures" to verify your identity before issuing credit in your name (as soon as one agency is notified, the others are notified to place fraud alerts as well). When you contact these agencies, you can also request that they provide a copy of your credit report. Review your reports carefully to ensure that the information contained in them is accurate. If you see anything on your credit reports or credit card account statements that appears incorrect, contact the credit reporting agency or your credit card provider, and report suspected incidents of identity theft to local law enforcement, the Attorney General, or the FTC. Even if you do not find any signs of fraud on your reports or account statements, the FTC and other security experts suggest that you check your credit reports and account statements periodically. You can keep the fraud alert in place at the credit reporting agencies by calling again after 90 days.

Placing a Security Freeze on Your Credit Report

You can also ask these same credit reporting agencies to place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. Please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. If you want to have a security freeze placed on your account, you must make a request in writing by certified mail to the reporting agencies. The reporting agencies will ask you for certain information about yourself. This will vary depending on where you live and the credit reporting agency, but normally includes your

MANDARIN ORIENTAL
THE HOTEL GROUP SM

name, social security number, date of birth, and current and prior addresses (and proof thereof), and a copy of government-issued identification.

The cost to place, temporarily lift, or permanently lift a credit freeze varies by state, but generally, the credit reporting agencies will charge $5.00 or $10.00, unless you are the victim of identity theft who has submitted a copy of a valid investigative or incident report, or complaint with a law enforcement agency, in which case under many state laws it is free. You have the right to a police report under certain state laws.

Further Information About How to Avoid Identify Theft and Report Incidents of Fraudulent Activity

If you detect any unauthorized charges on your credit card, we strongly suggest that you contact your card issuer by calling the toll-free number located on the back of your card or on your monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. You should tell your card issuer that your account may have been compromised and review all charges on your account for potentially fraudulent activity. We also recommend that you change your card web account password immediately when you discover unauthorized charges.

Finally, the FTC, your Attorney General, and the major credit reporting agencies listed above can provide additional information on how to avoid identity theft, how to place a fraud alert, and how to place a security freeze on your credit report. You can contact the FTC on its toll-free Identity Theft helpline: 1-877-438-4338. The FTC's website is located at http://www.ftc.gov/idtheft and its address is Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. In Maryland, you can reach the State Attorney General's office by phone at (888) 743-0023. Its website is http://www.oag.state.md.us/. In North Carolina, you can reach the State Attorney General's office by phone at (919) 716-6400. Its website is http://www.ncdoj.gov. Their mailing addresses are:

Douglas F. Gansler
Attorney General of the State of Maryland
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Roy A. Cooper
Attorney General of the State of North Carolina
Consumer Protection Division, Attorney General's Office
Mail Service Center 9001
Raleigh, NC 27699-9001

Once again, we wish to express our regret for this incident. We remain committed to delivering exceptional customer service, including protecting our guests' most personal information. If you have any questions about this notice or this incident or require further assistance, you can reach us at (877) 202-4625.

Yours sincerely,

Jan D. Goessing

Executive Vice President, Operations Director - The Americas