news release

MANDARIN ORIENTAL
THE HOTEL GROUP

# Press Release And Notice Regarding Mandarin Oriental Credit Card Breach

**July 10, 2015** – Earlier this year, Mandarin Oriental discovered a malware attack on our credit card systems in a number of our hotels listed below. In response, we issued a public statement on our website to alert guests to the attack so they could take proactive measures to monitor their credit card activity. We also immediately engaged law enforcement, cyber-forensic specialists, and appropriate credit card companies to coordinate investigation efforts and to take further steps to assist our guests. After a thorough investigation, we now know more about the incident and are notifying affected guests. We have established a call center that is prepared to address any questions our guests may have about the breach. We regret that this incident occurred and are sorry for any inconvenience it may cause. We take the safety and security of our guests and their personal information very seriously, and the trust our guests place in us remains an absolute priority.

From our investigation, it appears that a hacker used malware to obtain access to certain credit card systems in a number of Mandarin Oriental hotels. We believe this hacker may have used the malware to acquire the names and credit card numbers of guests who used a credit card for dining, beverage, spa, guest rooms, or other products and services at the following Mandarin Oriental properties during these time periods; we have not, however, found any evidence of acquisition or misuse of credit card pin numbers or security codes, or any other personal guest data:

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

Since we were first alerted to this attack, we have been investigating this incident across multiple countries and properties, and working in coordination with law enforcement and the credit card companies. We have timed this notice to avoid disrupting or impeding their concurrent investigations. We have also taken comprehensive steps to ensure that the malware has been removed and that the hacker is no longer in our systems.

In some instances, a credit card company may have already replaced the potentially affected credit card if it determined that the guest was at risk. We encourage potentially affected guests to remain vigilant for instances of fraud and identity theft, and to regularly review and monitor relevant account statements and credit reports to ensure the information contained in them is accurate. If any unauthorized charges on credit or debit card(s) are detected, guests should contact their card issuer. If anything is seen that is incorrect on credit reports, guests should contact the credit reporting agency. Suspected incidents of identity theft should be reported to local law enforcement. Even if no signs of fraud are found on reports or account statements, security experts suggest that credit reports and account statements should be checked periodically.

-more-

**FOR UNITED STATES RESIDENTS**

***Fraud alert***

Individuals who believe they may be affected by this incident may elect to place a fraud alert with the major credit reporting agencies on their credit files. Their contact information is as follows:

| | | | |
|---|---|---|---|
| Equifax | Equifax Information Services LLC<br>P.O. Box 105069<br>Atlanta, GA 30348-5069 | 800-525-6285 | www.equifax.com |
| Experian | Experian Fraud Reporting<br>P.O. Box 9554<br>Allen, Texas 75013 | 888-397-3742 | www.experian.com |
| TransUnion | TransUnion LLC<br>P.O. Box 6790<br>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 their identity before issuing credit in their name (as soon as one agency is notified, the others are notified to place fraud alerts as well). Individuals can also request these agencies to provide them with a copy of their credit report. The fraud alert can be kept in place at the credit reporting agencies by calling again after 90 days.

***Security freeze***

Individuals can also ask these same credit reporting agencies to place a security freeze on their credit report. A security freeze prohibits a credit reporting agency from releasing any information from an individual's credit report without written authorization. Placing a security freeze on the credit report may delay, interfere with, or prevent the timely approval of any requests from the individual concerned. This may include requests for new loans, credit, mortgages, employment, housing or other services. If individuals want to have a security freeze placed on their account, they must make a request in writing by certified mail to the reporting agencies. The reporting agencies will ask for certain personal information, which will vary depending on where the individual lives and the credit reporting agency. It normally includes 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. Generally, the credit reporting agencies will charge $5.00 or $10.00. However, if the individual is the victim of identity theft and has a copy of a valid investigative or incident report, or complaint with a law enforcement agency, in many states it is free. Individuals have the right to a police report under certain state laws.

***Information about how to avoid identity theft***

Besides local law enforcement, individuals can also report suspected instances of identity theft to their Attorney General, or the Federal Trade Commission (the "FTC"). The FTC, state Attorneys General, and major credit reporting agencies can provide additional information on how to avoid identity theft, how to place a fraud alert, and how to

place a security freeze on credit reports. The FTC can be contacted on its toll-free Identity Theft helpline: 1-877-438-4338. The FTC's website is http://www.ftc.gov/idtheft. Its address is Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. In Maryland, the State Attorney General's office can be reached by phone at (888) 743-0023. Its website is http://www.oag.state.md.us/. In North Carolina, the State Attorney General's office can be reached 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

***Further information***

Consumers who have questions about this notice or this incident, or have requests for further assistance should call: (877) 202-4625 (for calls from the United States and Canada); 800-87777888 (for calls from the United Kingdom); 0800561270 (for calls from Switzerland); 800901342 (for calls from Hong Kong); and 606-878-4212 (for all other calls). Please use this reference number when calling: 6322070615.

For media enquiries please contact: Jamaal Mobley at +1 202 393 7337, Vanessa Gourlay at +852 3512 5000, or Dania Saidam at +44 020 7404 5959, or email us at mohg@brunswickgroup.com.

***Q&A***

**What happened?**
It appears that a hacker used malware to obtain access to certain credit card systems in a number of Mandarin Oriental hotels. We believe the hacker may have used this malware to acquire the credit card numbers of individuals who used a credit card for dining, beverage, spa, guest rooms, or other products and services at the affected Mandarin Oriental properties.

**Which hotels were affected and when?**
Our investigation indicates that malware was potentially used at the following Mandarin Oriental properties 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

**What did Mandarin Oriental do to respond to the attack?**
As soon as we discovered the malware, we issued a public statement on our website to alert guests to the incident so they could take proactive measures to monitor their credit card activity. At the same time, we launched a comprehensive cyber-forensic investigation and engaged with credit card companies and law enforcement.

We have also taken comprehensive steps to ensure the removal of the malware, to ensure the hacker is no longer in our systems, and to contain and remediate the incident. Since we were first alerted to this attack, we have been working in coordination with the credit card companies and law enforcement to investigate the matter, and have timed our notice now in order to avoid impeding their concurrent investigations.

**What personal information was affected?**
We found malware on our credit card systems. From our investigation, it appears the hacker may have used that malware to acquire the credit card numbers and, in some instances, the names of individuals who used a credit card for dining, beverage, spa, guest rooms, or products and other services at the affected Mandarin Oriental properties. The malware did not acquire the pin numbers or the 3- to 4- digit security code printed on the credit card, or any other personal guest data.

**Why did Mandarin Oriental have guests' personal information?**
Guest names and credit card numbers are used to secure hotel guest reservations, and to process purchases at various hotel outlets such as restaurants and spas. Based upon our forensic investigation, it appears this malware was designed to access the credit card numbers at the time of transaction as they were being transmitted.

**When and how did Mandarin Oriental learn about the malware attack?**
In late February 2015, we were alerted by our payment card processors that credit card systems at some of our hotels may have been the target of certain malicious activity. We immediately launched a comprehensive forensic investigation into the matter, working in coordination with law enforcement and the credit card companies. We also issued a public statement on our website to alert guests to the attack so they could take proactive measures to monitor their credit card activity.

**Who did this? Have they been caught?**
We do not know who is responsible for the intrusion. We understand that law enforcement is conducting an ongoing investigation into the matter.

**Is the personal information of your guests safe and how will you prevent this from happening in the future?**
We take seriously the security and protection of our guests' personal information. We have conducted a comprehensive forensic investigation of all potentially affected systems to ensure the malware has been removed and the incident remediated. We have taken steps across all Mandarin Oriental hotel properties to guard against the recurrence of such an attack and to further protect guest information.

**Who has been notified?**
We have notified all consumers who used a credit card at one of the affected Mandarin Oriental hotel properties during the relevant time periods through a press release issued to media outlets and posted on our website. We also issued a

letter directly to guests whose contact information we had, if we determined during forensic investigation that their credit card numbers may have been acquired without authorization. Additionally, we have engaged with law enforcement, the credit reporting agencies, the payment card companies, and other relevant regulatory authorities.

**If a Mandarin Oriental guest has more questions regarding this incident, who should they contact?**
Any guest that has further questions relating to this matter should call: (877) 202-4625 (for calls from the United States and Canada); 800-87777888 (for calls from the United Kingdom); 0800561270 (for calls from Switzerland); 800901342 (for calls from Hong Kong); and 606-878-4212 (for all other calls). Please use this reference number when calling: 6322070615.

-ends-