NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2732
david.navetta@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

September 25, 2015

By Certified Mail
Return Receipt Requested

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

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, the Trump Hotel Collection ("THC") to inform you of a potential security incident involving payment card information that may have affected some residents of New Hampshire. At this time, we have identified approximately three New Hampshire residents that may have been affected by this incident. THC is providing notice to these individuals and outlining some steps they may take to help protect themselves.

THC is providing notice of a security incident possibly affecting certain individuals who made payment card purchases at Trump International Hotel & Tower Las Vegas, located at 2000 Fashion Show Drive, Las Vegas, NV, 89109 and Trump International Waikiki, located at 223 Saratoga Road, Honolulu, HI 96815 (the "Hotels").

While the independent forensic investigator did not find evidence that information was taken from the Hotels' systems, it appears that there may have been unauthorized malware access to payment card information as it was inputted into the payment card systems. Payment card data (including payment card account number, card expiration date, security code, and cardholder name) of individuals who used a payment card at the Hotels between May 19, 2014, and June 2, 2015, may have been affected.

THC takes the privacy of personal information seriously. Immediately upon learning of a possible incident, THC notified the financial institutions, and engaged an outside forensic expert to conduct an investigation of the incident. As part of the investigation, THC has removed the malware, changed access credentials, and is in the process of reconfiguring various components of our network and payment systems to further secure our payment card processing systems. In addition, THC notified law enforcement, including the U.S. Secret Service and the Federal Bureau of Investigation, of the situation and THC will cooperate with

any investigation they conduct and assist in their efforts to catch the criminals that may have compromised our system and our customers' information.

Affected individuals are being notified via various channels including written letter, e-mail, website and media notice. The notifications include an offer for one year of complimentary identity protection and fraud resolution services. The notifications will be sent on or around September 25, 2015. A form copy of the notice being sent to affected New Hampshire residents is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2732 or david.navetta@nortonrosefulbright.com.

Very truly yours,

David Navetta
Partner
Co-Chair, Data Protection, Privacy & Access
to Information

DJN/kck
Enclosure

NORTON ROSE FULBRIGHT

[DATE]

[ADDRESS]

Dear [NAME],

On behalf of our client, The Trump Hotel Collection ("THC"), and as a precaution, we are providing notice of a security incident possibly affecting certain individuals who made payment card purchases at Trump International Hotel & Tower Las Vegas, located at 2000 Fashion Show Drive, Las Vegas, NV, 89109 (the "Hotel"). Although an independent forensic investigation has not conclusively determined that any particular customer's payment card information was taken from the Hotel's payment card system or misused as a result of the incident, we are providing this notice out of an abundance of caution to inform potentially affected customers of the incident and to call their attention to some steps they may choose to take to help protect themselves.

While the independent forensic investigator did not find evidence that information was taken from the Hotel's systems, it appears that there may have been unauthorized malware access to payment card information as it was inputted into the payment card systems. Payment card data (including payment card account number, card expiration date, security code, and cardholder name) of individuals who used a payment card at the Hotel between May 19, 2014, and June 2, 2015, may have been affected.

THC takes the privacy of personal information seriously. Immediately upon learning of a possible incident, THC notified the F.B.I. and financial institutions, and engaged an outside forensic expert to conduct an investigation of the incident. As part of the investigation, THC has removed the malware and is in the process of reconfiguring various components of our network and payment systems to further secure our payment card processing systems. THC is confident that customers can safely use payment cards at all of the properties managed by THC.

We want to make potentially affected customers aware of steps they can take to guard against identity theft or fraud. We recommend that you review your credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor your statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued your credit or debit card immediately. We also recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. Also, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

In addition, THC is offering one year of complimentary fraud resolution and identity protection services to customers who used a payment card at the Hotel between May 19, 2014, and June 2, 2015. These services are only available to U.S. residents. For more information about this incident and ways you can protect yourself, including eligibility and enrollment information about the complimentary identity protection services, contact us toll-free at 877-803-8586.

Norton Rose Fulbright

Information about Identity Theft Protection

We have engaged Experian®, the largest credit bureau in the U.S., to offer you complimentary fraud resolution and identity protection services for one year. If you are a victim of fraud, simply call Experian at **877-297-7780** by **December 31, 2015**, and a dedicated Identity Theft Resolution agent will help you. Please provide the following engagement number as proof of eligibility: **PC96712**. We also encourage you activate Experian's® ProtectMyID® Alert product, which helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. To enroll, visit **www.protectmyid.com/alert** by **December 31, 2015** and use the following activation code: [**ACTIVATION CODE**]. You may also enroll over the phone by calling **877-297-7780** between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays).

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies

Equifax (www.equifax.com)
P.O. Box 105851
Atlanta, GA 30348
800-685-1111

Fraud Alerts: P.O. Box 105069, Atlanta, GA 30348
Credit Freezes: P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
P.O. Box 105281
Atlanta, GA 30348
877-322-8228

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872