<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<date>>

NOTICE OF DATA BREACH

Dear <<Name 1>>:

Drury Hotels values the relationship we have with our guests and understands the importance of protecting their information. We are writing to inform you of a security incident one of our service providers informed us of that may involve some of your information. This notice explains the incident, the measures we have taken in response, and some additional steps you may consider taking.

What Happened?
For most hotels, there are two ways to make a reservation – directly with the hotel or indirectly through third-party online booking websites (websites run by other companies that compare rooms and rates at different hotels). For reservations that are made through online booking websites, many hotels use a technology service provider to collect the reservation data from the online booking company and enter it into the hotel's property management system. On March 26, 2019, we were notified by the company that provides that service to us and other hotel companies that it was conducting an investigation to determine if there had been unauthorized access to its network. The service provider reported that it had hired a cybersecurity firm to conduct an investigation. Since then Drury Hotels has worked closely with the service provider to get updates on its investigation.

The service provider initially advised us that the unauthorized access to transaction records related to reservations in its network began on December 29, 2017 and ended on March 13, 2019. We previously notified the guests whose transaction records were sent through the service provider's network between those dates. Despite the service provider's assurances that the unauthorized access was limited to that time frame, it has now informed us that transactions between December 28, 2017 and June 2, 2019 are involved.

After the service provider informed Drury Hotels that the time frame of the incident may have changed, Drury Hotels contacted the cybersecurity firm engaged by the service provider to determine what occurred. Drury Hotels received the findings and answers to questions needed to clarify the findings on September 23, 2019.

What Information Was Involved?
A transaction record related to a reservation you made for a stay at a Drury Hotel through a third-party's online booking website during the revised time frame was involved. The information in the transaction record included your name, address, payment card number, expiration date, and the card's external verification code. Some transaction records also included email addresses. Specific details regarding the reservation itself were not involved.

Reservations that were made directly with Drury Hotels (by calling Drury Hotels or using our website or mobile app) were not involved in this incident.

What You Can Do.
We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank that issued your card. If reported timely, payment card network rules generally provide that cardholders are not responsible for unauthorized charges. Information on additional steps you can take can be found on the following pages.

What We Are Doing.
We regret that this incident occurred and apologize for any inconvenience. Since then Drury Hotels has worked closely with the service provider to get updates on its investigation. Drury Hotels received confirmation from the service provider and the cybersecurity firm it engaged that it has undertaken measures to stop this incident and prevent something like this from happening again. We will continue to work with the service provider to identify the security enhancements it is implementing.

For More Information.
If you have any questions about this matter, please call (800) 382-6291, Monday to Friday, from 8:00 a.m. to 8:00 p.m., Eastern Time.

Sincerely,

Ryan Schlimpert
Vice President/Chief Information Officer

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft