



August 6, 2010

By E-Mail and First Class Mail

Maryland Office of the Attorney General
Attn: A. Hugh Williams
200 St. Paul Place
Baltimore, MD 21202

Robert D. Forbes
Attorney at Law
d 310.284.4545
f 310.557.2193
rforbes@proskauer.com
www.proskauer.com

Re: Destination Hotels & Resorts Data Breach

Dear Mr. Williams:

I write on behalf of my client, Destination Hotels & Resorts, Inc. ("DHR"), to provide an update to my letter dated July 20, 2010 (enclosed). Further investigation revealed that the computer systems of one of our New York properties was accessed as early as April 2009. As a result of this incident, credit or debit card information, including card numbers and expiration dates, may have been subjected to unauthorized access by third parties. It is DHR's continued belief that no other personal information, such as Social Security numbers, was stolen.

This incident affected 22 DHR properties in Arizona, California, Colorado, New Jersey, New Mexico, New York, North Carolina, Oregon, South Carolina, Texas, Vermont, and Washington. There were no affected properties in the State of Maryland.

DHR took action by immediately notifying the payment card processing companies that this payment card information may have been subjected to compromise as a result of the breach. DHR also engaged a specialized computer forensics company to conduct a comprehensive investigation of the computer security breach. DHR has notified all affected individuals through first class mail, e-mail, and/or substitute notice and has provided them with precautionary information and measures they can take to safeguard their information. These notifications began mailing on or about July 20, 2010. A copy of the form of notice to affected individuals in your state is attached to my letter of July 20, 2010 for your reference.

If you have any questions or need further information regarding this incident, please call me.

Best regards,

Robert D. Forbes

Enclosure



July 20, 2010

By Facsimile and Mail

Maryland Office of the Attorney General
Attn: A. Hugh Williams
200 St. Paul Place
Baltimore, MD 21202

Robert D. Forbes
Attorney at Law
d 310.284.4545
f 310.557.2193
rforbes@proskauer.com
www.proskauer.com

Re: Destination Hotels & Resorts Data Breach

Dear Mr. Williams:

I write on behalf of my client, Destination Hotels & Resorts, Inc. ("DHR"), to inform you of a recent incident involving the personal information about some of your state's residents. Between January 1 and June 15 of this year the computer systems of some DHR hotels were accessed without authorization. As a result of this incident, credit or debit card information, including card numbers and expiration dates, may have been subjected to unauthorized access by third parties. At this time DHR has no reason to believe that any other personal information, such as Social Security numbers, was stolen.

This incident affected 22 DHR properties in Arizona, California, Colorado, New Jersey, New Mexico, New York, North Carolina, Oregon, South Carolina, Texas, Vermont, and Washington. There were no affected properties in the State of Maryland. Approximately 1,354 individuals affected by this incident are residents of your state.

DHR took action by immediately notifying the payment card processing companies that this payment card information may have been subjected to compromise as a result of the breach. DHR also engaged a specialized computer forensics company to conduct a comprehensive investigation of the computer security breach. As a result of this quick response, DHR has no reason to believe that any payment card data is currently at risk within any DHR hotels. Nonetheless, as a precaution, DHR is notifying all affected individuals via written letter through first class mail, and providing them with precautionary information and measures they can take to safeguard their information. These notifications will begin mailing on or about July 20, 2010. A copy of the form of notice to affected individuals in your state is attached for your reference.

If you have any questions or need further information regarding this incident, please call me.

Best regards,

Robert D. Forbes



July 20, 2010

Page 2

[Name and Mailing address from mailing list]

Re: Notice Regarding Theft of Payment Card Information

Dear Valued Guest:

Destination Hotels & Resorts values your business and respects the privacy of your information, which is why we wish to inform you that between January 1 and June 15 of this year the computer systems of some Destination hotels were accessed without authorization. This unauthorized access was in violation of both civil and criminal laws. Destination has been coordinating with law enforcement, including the FBI, to assist in the investigation of this incident. The hotels that we believe were affected include those listed on the other side of this letter.

As a result of this unfortunate incident, your credit or debit card information, including your card number and expiration date, may have been subjected to unauthorized access by third parties. At this time we have no reason to believe that any other personal information, such as your Social Security number, was stolen. Destination Hotels & Resorts took action immediately by engaging a specialized computer forensics company to conduct a comprehensive investigation of the computer security breach. We are also taking several steps to enhance existing security controls. As a result of the quick response, we have no reason to believe that your payment card data is currently at risk within any Destination hotels.

Please know that we are committed to rectifying this situation and to helping prevent the misuse of your payment card information. We have notified the payment card processing companies that your payment card information may have been subjected to compromise as a result of the breach. In addition, please see the enclosure with this letter for information about additional steps you can take to protect yourself from identity theft.

Other than in the form of this written letter, Destination Hotels & Resorts will not initiate further contact with you about this incident, either by phone or in writing, and will not ask you to confirm any sensitive personal information, such as your Social Security number. If you do happen to receive a communication with a request like this, it is not from Destination Hotels & Resorts, and you should not provide any information in this regard.

Destination Hotels & Resorts regards the privacy of consumer information with the utmost of importance. To that end, Destination Hotels & Resorts has numerous security measures in place to safeguard our customers' payment card information. Further, Destination Hotels & Resorts continues to implement additional security measures in order to meet the demands of today's computer based society.

If there is anything we can do to assist you further, please feel free to call us at 1-800-XXX-XXXX, or contact us at our mailing address below.

We truly regret any inconvenience for this situation.

Sincerely,

Charles S. Peck
President

List of Destination Properties

The Carolina Inn
The Driskill Hotel
Estancia La Jolla Hotel & Spa
Hamilton Park Hotel & Conference Center
Hotel ICON
Inn and Spa at Loretto
The Inverness Hotel and Conference Center
L'Auberge Del Mar Resort and Spa
Manor Vail Lodge
Miramonte Resort & Spa
Resort at Squaw Creek
Paul J. Rizzo Conference Center
Skamania Lodge
Stowe Mountain Lodge
Suncadia Resort
Tarrytown House Estate & Conference Center
Tempe Mission Palms Hotel and Conference Center
Vail Cascade Resort & Spa
Wild Dunes Resort
Destination Resorts Snowmass
Destination Resorts Vail
The Gant

IMPORTANT STEPS TO HELP PREVENT FRAUD

1. **Carefully review your debit or credit card account statements and report any unauthorized transactions.** You should regularly review your accounts to look for unauthorized or suspicious activity. You may also want to notify your financial institution(s) and credit card companies that you received this notice. This will tell them that your information may have been viewed or accessed by an unauthorized party. You may also want to request a new debit or credit card from these institutions if one has not already been issued to you.
2. **Consider contacting the fraud department at the three major credit bureaus listed below and ask them to place a "fraud alert" on your credit file.** A fraud alert tells creditors to contact you before they open any new credit accounts. To place a fraud alert on your credit file, contact one of the three national credit bureaus at the numbers provided below.

Equifax
(800) 685-1111
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374-0241

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

TransUnion
(800) 916-8800
www.transunion.com
P.O. Box 6790
Fullerton, CA 92834-6790

3. **Obtain a copy of your credit report from each of the three major credit reporting agencies and review them to be sure they are accurate and include only authorized accounts.** You are entitled to one free copy of your report every 12 months. To order your report, visit www.annualcreditreport.com, or call toll-free (877) 322-8228, or complete an Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 (you can print a copy of the request form at <http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtm>). Carefully review your credit reports to verify that your name, address, account, and any other information are accurate and notify the credit reporting agencies of any errors you detect, and about any accounts you did not open or inquiries from creditors you did not initiate. In addition to your free credit report, you can also purchase a copy of your credit report by contacting one of the three national credit reporting companies listed above.
4. **Contact the Federal Trade Commission ("FTC") to obtain additional information about how to protect against identity theft.** The FTC is a good resource for general questions about identity theft. As a Maryland resident, you may also obtain additional information from your state's Attorney General.

MD Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

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

5. **We recommend that you remain vigilant over the next 12 to 24 months and report any suspected identity theft or other misuse of personal information immediately to the proper law enforcement authorities.** You have the right to obtain a police report if you are the victim of identity theft.