

April 16, 2018

**VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
AND FEDERAL EXPRESS**New Hampshire Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301**Re: Notification of Potential Data Security Incident**

Dear Attorney General MacDonald:

We represent World Travel Holdings, Inc. ("WTH") in connection with a recent incident that may have impacted the personal information of twelve (12) New Hampshire residents. WTH, on behalf of itself and its private label partners identified below, is reporting a potential unauthorized access to computerized data containing personal information of those twelve (12) New Hampshire residents pursuant to N.H. REV. STAT. ANN. § 359-C:20.

The investigation of this incident is ongoing, and this notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. WTH is advising you of this incident based on the information available to date. By providing this notice, WTH does not waive any potential rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction in connection with this incident.

Background of the Incident

WTH is a Delaware corporation with its principal place of business at 100 Fordham Road, Building C, Wilmington, Massachusetts 01887. WTH is a vacation, travel and cruise company that serves its customers through a variety of brands, both directly (including through subsidiary and affiliated entities) and through private label partnerships with other leisure travel providers. For purposes of this notice, these brands consist of the following:

WTH Brands

Brand	Potentially Affected Individuals in New Hampshire
Cruises.com	2
CruiseOne/Dream Vacations	1

Vacation Outlet	2
World Travel Holdings	1
Subtotal WTH Brands	6

Private Label Partner Brands

Brand	Potentially Affected Individuals in New Hampshire
BJ's Travel (owned by BJ's Wholesale Club, Inc.)	6
Subtotal Private Label Partner Brands	6
Total	12

Certain of the products and services WTH offers its customers, including customers of its partner brands, are provided through software made available by third-party application service providers, including Orbitz Worldwide, LLC ("Orbitz"). Orbitz notified WTH on March 19, 2018 that certain travel reservations made by or on behalf of WTH's customers or customers of its partner brands may have been affected by a data security incident affecting a legacy Orbitz travel booking platform (the "platform"). Orbitz has advised that while conducting an investigation of the platform, Orbitz determined on March 1, 2018 that there was evidence suggesting that, between October 1, 2017 and December 22, 2017, an attacker may have accessed certain personal information stored on the platform. Orbitz has reported taking immediate steps to investigate the incident and enhance security and monitoring of the affected platform, and making every effort to remediate the issue, including taking swift action to eliminate and prevent unauthorized access to the platform. Orbitz has advised that it does not have direct evidence that personal information was actually taken from the platform.

Orbitz has determined that the personal information that was likely accessed may have included the full name, payment card information, date of birth, phone number, email address, physical and/or billing address and gender of individuals. The Orbitz investigation to date has not found any evidence of unauthorized access to other types of personal information, including passport and travel itinerary information. Additionally, for U.S. customers, Orbitz has determined that Social Security numbers were not involved in this incident, because they are not collected or held on the platform.

Notice to the New Hampshire Residents

During the week of April 16, 2018, WTH will notify the twelve (12) affected New Hampshire residents. Enclosed is a copy of the notice that is being sent to the impacted individuals. The "Brand" or "Partner" space in each of these letters will be filled in with the relevant brand information tabulated above for each affected New Hampshire resident. Additionally, as stated in the letter template, Orbitz has

Gordon J. MacDonald, Attorney General

April 16, 2018

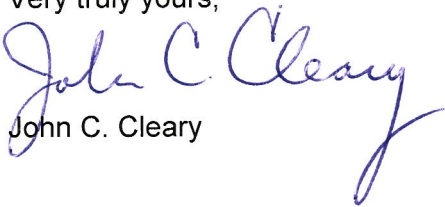
Page 3

has arranged to offer one (1) year of complimentary credit monitoring and identity theft protection services through AllClear ID to affected New Hampshire residents, and Orbitz has established an inquiry line (1-855-828-5646) and website address (<https://orbitz.allclear.com/>) that affected New Hampshire residents can utilize to ask questions and to receive further information.

Contact Information

Please contact me if you have any questions or if I can provide you with any further information concerning this matter. Thank you.

Very truly yours,



John C. Cleary

Enclosure

cc: Jamie Cash, Senior Vice President, Technology, World Travel Holdings, Inc.

**SAMPLE NOTIFICATION LETTER FOR AFFECTED PARTNER CUSTOMERS:
U.S. CUSTOMERS**

A sample notification letter is provided below that you may choose to adapt for notifying your affected customers who are residents of the United States. If you choose to utilize this letter, please note that legal requirements may apply differently to each business in different jurisdictions and the letter may require tailoring to your specific circumstances.

[Insert Letterhead with Name, Address, and Contact Information of Partner Providing Notice]

[Date]

[Recipient name]

[Recipient street address]

[Recipient state and ZIP]

NOTICE OF DATA BREACH

We recently learned that certain travel reservations you made through [PARTNER NAME], which was powered by Orbitz, may have been affected by a data security incident affecting a legacy Orbitz travel booking platform (the “platform”). We are contacting you because we believe it may have affected some of your personal information submitted for certain purchases made from [IMPACTED DATES].

What Happened?

While conducting an investigation of the platform, Orbitz determined on March 1, 2018 that there was evidence suggesting that, between October 1, 2017 and December 22, 2017, an attacker may have accessed certain personal information stored on this consumer and business partner platform. Orbitz took immediate steps to investigate the incident and enhance security and monitoring of the affected platform, and made every effort to remediate the issue, including taking swift action to eliminate and prevent unauthorized access to the platform. To date, we do not have direct evidence that this personal information was actually taken from the platform.

What Information Was Involved?

On March 1, 2018, Orbitz determined that the personal information that was likely accessed may have included your full name, payment card information, date of birth, phone number, email address, physical and/or billing address, and gender.

What Information was *Not* Involved?

The Orbitz investigation to date has not found any evidence of unauthorized access to other types of personal information, including passport and travel itinerary information. Additionally, for U.S. customers, Orbitz determined that Social Security numbers were not involved in this incident, because they are not collected nor held on the platform.

What We Are Doing

Orbitz considers the security of all personal information as a top priority. Orbitz took immediate steps to investigate the incident and enhance security and monitoring of the affected platform. As part of the Orbitz investigation and remediation work, Orbitz brought in a leading third party forensic investigation firm and other cybersecurity experts, began working with law enforcement, and took measures to effectively prevent any unauthorized access and enhance security. Upon determining that the attack may have resulted in access to certain personal information, it also started working immediately to notify potentially impacted customers and business partners.

Orbitz is offering you and other affected customers one year of complimentary credit monitoring and identity protection service in countries where available. You may sign up for this service by following the instructions included in **Attachment A**.

What You Can Do

Regardless of whether you elect to enroll in the credit monitoring and identity protection service, Orbitz recommends that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please contact your financial institution or call the number on the back of your payment card. **Attachment B** contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information

If you have any questions about this notice or the incident, please call 1-855-828-5646 (toll-free U.S.) or 1-512-201-2217 (International), or visit <https://orbitz.allclearid.com/>. Or you can contact us on [**PARTNER CONTACT DETAILS**].

ATTACHMENT A

For affected U.S. customers, the following services are available:

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-828-5646 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-828-5646 using the following redemption code: [REDEMPTIONCODE].

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

ATTACHMENT B

Additional Information

To protect against possible fraud, identity theft or financial loss, we encourage you to remain vigilant, review your account statements, and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit reporting agencies and additional information about steps you can take to obtain a free credit report and to place a fraud alert, credit freeze, or credit lock on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your State's attorney general, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit reporting agencies. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three credit reporting agencies below:

Equifax:
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
1-888-766-0008
www.equifax.com

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
TransUnion LLC
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting the three major credit reporting agencies at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days, but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, 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.

To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years. The cost to place a credit freeze is typically between \$5.00 and \$10.00 each time you place a freeze, but may vary by jurisdiction. Certain jurisdictions may also permit a credit reporting agency to charge you similar fees to lift or remove the freeze. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a credit freeze.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or <http://www.oag.state.md.us>.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or <http://www.ncdoj.gov>.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or <http://www.riag.ri.gov/>. You may also file a police report by contacting local or state law enforcement agencies.