March 20, 2018

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Breach Pursuant to N.H. Rev. Stat. § 359-C:20

To Whom It May Concern:

In accordance with the above-referenced provision of New Hampshire law, I write to inform you of a data security incident affecting residents of New Hampshire.

While conducting an investigation of a legacy Orbitz travel booking platform (the "platform"), we determined on March 1, 2018 that there was evidence that, between October 1, 2017 and December 22, 2017, an attacker may have accessed personal information, stored on the platform, that was submitted for certain purchases made between January 1, 2016 and June 22, 2016. The platform is provided directly to consumers ("direct consumers") as well as to business partner customers. We 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.

On March 1, 2018, we determined that the personal information that was likely accessed may have included full name, payment card information, date of birth, phone number, email address, physical and/or billing address, and gender. Our investigation to date has not found any evidence of unauthorized access to other types of personal information, including passport and travel itinerary information. Additionally, Social Security numbers were not involved in this incident, as these are not collected through nor held on the platform.

Upon learning of the incident, Orbitz took immediate steps to protect consumers by investigating the incident and enhancing security and monitoring of the affected platform. As part of our investigation and remediation work, we 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, we also started working immediately to notify potentially impacted direct consumers and business partners whose customers used the platform.

We plan to notify approximately 1,523 potentially affected direct consumers who are residents of New Hampshire. Enclosed is a copy of the notification letter that will be sent to affected U.S. direct consumers via first-class mail between March 22 and 23, 2018. For certain affected direct consumers for whom we have an email address and not a payment billing address, this notification will be provided via email. We have also issued a media advisory explaining the incident to the general public and established a public website (orbitz.allclearid.com) to provide additional details

found in the notification letters. We plan to provide notices of this incident to the three major credit reporting agencies on March 21, 2018.

The notification to individuals includes (1) a description of the incident and the type of personal information at issue; (2) the actions taken by Orbitz to protect personal information from further unauthorized access; (3) Orbitz's address and a toll-free phone number to call for further information and assistance; (4) information on how the individual may enroll in free credit monitoring and other complimentary services arranged by Orbitz; (5) information about how to place a fraud alert or security freeze on a credit report; (6) the toll-free numbers and addresses for the major consumer reporting agencies; (7) the toll-free number, address, and website for the Federal Trade Commission, and a statement that individuals can obtain information on identity theft from this source; and (8) advice that directs the individual to remain vigilant by reviewing account statements and monitoring free credit reports.

In addition to notifying direct consumers, we have notified affected business partners and will make available the following information and services to each partner whose customers' information may have been affected by this incident: a full list of impacted customers; consumer notice support by AllClear ID, which includes logistical support for printed notifications, a customer notification template, and a centralized call center to which partners can direct their customers who may have questions; talking points and frequently asked questions to assist partners in their own discussions with their customers; and one year of credit monitoring and identity protection service in countries where the service is available for affected customers from our providers AllClear ID and Experian. These partners may choose to notify regulators and affected individuals independently.

If you have any questions or need further information regarding this incident, please contact Cathy Bump at cathybump@orbitz.com.

Sincerely,

Cathy Bump
Global Privacy Director
500 W. Madison Street, 7th Floor
Chicago, IL 60661
(425) 679-3610
cathybump@orbitz.com

Enclosure

ORBITZ

Processing Center • P.O. BOX 141578 • Austin, TX 78714

47740
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

March 22, 2018

NOTICE OF DATA BREACH

We are writing to share important information about a data security incident that may have affected some of your personal information.

First and foremost, we want to reinforce that keeping the personal data of our customers safe and secure is very important to us, and we deeply regret this occurred. We can assure you that as soon as we determined there was likely unauthorized access to some personal information, we took swift action to address the issue and protect our customers. You should know that the current Orbitz.com website was not in any way involved in this incident.

What Happened?

While conducting an investigation of a legacy Orbitz travel booking platform (the "platform"), we determined on March 1, 2018 that there was evidence suggesting that, between October 1, 2017 and December 22, 2017, an attacker may have accessed personal information, stored on this consumer and business partner platform, that was submitted for certain purchases made between January 1, 2016 and June 22, 2016. We 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.

What Information Was Involved?

On March 1, 2018, we 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?

Our investigation to date has not found any evidence of unauthorized access to other types of personal information, including passport and travel itinerary information. Additionally, we can assure you that Social Security numbers were not involved in this incident, as these are not collected nor held on the platform.

What We Are Doing

We consider the security of all personal information as a top priority. We took immediate steps to investigate the incident and enhance security and monitoring of the affected platform. As part of our investigation and remediation work, we 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, we also started working immediately to notify potentially impacted customers and business partners.

We are 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, we recommend 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 1-855-828-3959 (toll-free U.S.) or 1-512-201-2214 (International), or visit orbitz.allclearid.com.

We believe travel is one of life's greatest pleasures and we are committed to maintaining your trust so you will book with us again with confidence. We sincerely regret that this incident occurred, and we apologize for any inconvenience that may have been caused by this incident.

ATTACHMENT A

The following services are available for 12 months from the date of enrollment:

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-828-3959 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 1-855-828-3959 using the following redemption code: Redemption Code.

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:	Experian:	TransUnion:
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: Consider contacting the three major credit reporting agencies at the addresses above 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.