

VIA OVERNIGHT DELIVERY

April 5, 2018

Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH, 03301

RECEIVED

APR 06 2018

CONSUMER PROTECTION

Re: Incident Notification

Dear Sir/Madam:

This firm represents Interval International, Inc. (“**Interval**”). We are writing to inform you of an incident involving the inadvertent disclosure of certain information related to New Hampshire residents by a third-party vendor to Interval, Orbitz Worldwide, LLC (“**Orbitz**”). Although the information that may have been accessed does not trigger any notification requirements under N.H. Rev. Stat. Ann. §359-C:20, Interval has elected to notify all consumers that may have been affected by this incident, and accordingly providing the information to you as well. Orbitz is providing all affected consumers with access to credit monitoring services, and notification to consumers was necessary in order to provide them with instructions on how to sign up for the services.

Interval had an established business relationship with Orbitz to provide travel reservation services through the Orbitz Partner Network link on IntervalWorld.com (“**Orbitz Partner Link**”). On or about March 21, 2018, Orbitz advised Interval that certain travel reservations made through the Orbitz Partner Network Link may have been affected by a data security incident during the period between January 1, 2016 and December 2, 2017. Following an examination of forensic evidence, Orbitz determined that an unauthorized party gained access to a legacy Orbitz travel booking platform (the “**Platform**”) that permitted unauthorized access to certain payment card information, as well as certain reservation information, for a subset of travel reservations processed through the Platform.

According to Orbitz, the unauthorized party may have been able to access information for certain travel reservations including cardholder name; payment card number; and card expiration date. The unauthorized party may have also been able to access certain information such as email, date of birth, phone number, physical and billing address, and gender. It is important to note that based upon the information provided to Interval by Orbitz, these files **did not** contain a security code, access code, password, CVV data, magnetic strip data, passport numbers, or driver’s license numbers. Since the unauthorized party was not able to access credit or debit card number *in combination with* any required security code, access code, or password, no personal information under N.H. Rev. Stat. Ann. §359-C:20 was breached.

Holland & Hart LLP Attorneys at Law

Phone (303) 473-2700 Fax (303) 473-2720 www.hollandhart.com

One Boulder Plaza 1800 Broadway Suite 300 Boulder, CO 80302

Alaska Colorado Idaho Montana Nevada New Mexico Utah Washington, D.C. Wyoming

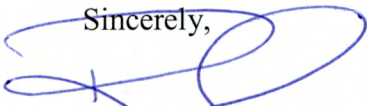
Orbitz has advised Interval that promptly after learning of the incident, Orbitz engaged a leading third party forensic investigation firm and other cybersecurity experts, has alerted federal law enforcement agencies, and has provided notice to the credit payment processors for impacted consumers. Upon determining that the attack may have resulted in access to certain personal information, it also started working immediately to notify potentially impacted business partners, such as Interval.

Orbitz has represented to Interval that it has enhanced its security around the affected Platform and is monitoring the system activity to further detect and prevent unauthorized access. Please also note that the Orbitz Partner Network Link is no longer available on IntervalWorld.com.

Interval has sent written notification via U.S. Mail to approximately 3 New Hampshire residents on or about April 4, 2018, in substantially the same form as the letter attached hereto. Notice is being provided as expeditiously as practicable and without unreasonable delay. Orbitz is offering the affected individuals credit monitoring at no charge for a period of 12 months.

If you have any questions or need further information regarding this incident, please contact the undersigned at 303.473.4808 or rdspilde@hollandhart.com.

Sincerely,



Richard Spilde, Jr., P.C.
Holland & Hart LLP

RDS/
Enclosure



April 4, 2018

First Name Last Name
Delivery Address
Alternate 1 Address
City St ZIP+4

NOTICE OF DATA BREACH

Dear Valued Customer:

We are writing to you because of an incident involving unauthorized access to customer information associated with your travel reservation(s) made through the Orbitz Partner Network link on the IntervalWorld.com website. The privacy and protection of our customers' information is a matter we take very seriously, and we recommend that you closely review the information provided in this letter for some steps that you may take to protect yourself against potential misuse of your information.

What Happened?

On or about March 21, 2018, Orbitz Worldwide, LLC ("Orbitz") advised Interval International ("Interval") that certain travel reservations made through the Orbitz Partner Network link on IntervalWorld.com may have been affected by a data security incident. Following an examination of forensic evidence, Orbitz determined that an unauthorized party gained access to a legacy Orbitz travel booking platform (the "Platform") that permitted unauthorized access to payment card information, as well as certain reservation information, for a subset of travel reservations processed through the Platform.

The investigation determined that between October 1, 2017 and December 22, 2017, a third party obtained unauthorized access to payment card and other information for reservations processed between January 1, 2016 and December 2, 2017. However, please be advised that, to date, Orbitz has not provided Interval any direct evidence that personal information was actually taken from the Platform.

What Information Was Involved?

The unauthorized party may have been able to access the payment card information associated with your travel reservation(s), including cardholder name and card number. The unauthorized party may have also been able to access certain information regarding you and other travelers on your reservation, such as email address, date of birth, phone number, physical and/or billing address, and gender. It is important to note that according to Orbitz, the files accessed **did not** contain CVV data, magnetic strip data, passport numbers, or driver's license numbers. As a result, we have no reason to believe that any of this type of data was accessed, if you were required to provide it in conjunction with your reservation.

What We Are Doing

The Orbitz Partner Network link is no longer available on IntervalWorld.com.

Orbitz reports that it took immediate steps to investigate the incident and to enhance the security and monitoring of the affected Platform. Orbitz also states that it has brought in a leading third party forensic investigation firm and other cybersecurity experts, has alerted federal law enforcement agencies, and has provided notice to the credit payment processors for impacted consumers. Upon determining that the attack may have resulted in access to certain personal information, it also started working immediately to notify potentially impacted business partners, such as Interval.

*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 **Addendum A**.*

What You Can Do

Regardless of whether you elect to enroll in the credit monitoring and identity protection service, you should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported.

In addition, you may contact the Federal Trade Commission (FTC) or law enforcement, such as your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580
(877) IDTHEFT (438-4338); <https://www.identitytheft.gov/>

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the credit reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at <https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting agencies to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days. An extended alert stays on your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report.

Also, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, 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. The credit reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide credit reporting agencies at:

Equifax
P.O. Box 105788
Atlanta, GA 30348
(800) 525-6285
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(800) 680-7289
www.transunion.com

Please see the insert for certain state-specific information.

For More Information

We apologize for any inconvenience caused by this incident. 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/>. For questions directed to Interval, please call 1-800-252-5121.

Sincerely,

INTERVAL INTERNATIONAL, INC.

Addendum 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 property 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 <https://orbitz.allclearid.com> or by phone by calling **1-855-828-3959**.

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.

IF YOU ARE AN IOWA RESIDENT:

You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

IF YOU ARE A MARYLAND RESIDENT:

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

IF YOU ARE A NEW MEXICO RESIDENT:

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. the unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. proper identification to verify your identity;
3. information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
4. payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies using the contact information provided in the enclosed letter.

IF YOU ARE A NORTH CAROLINA RESIDENT:

You may obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
<http://www.ncdoj.gov>

IF YOU ARE AN OREGON RESIDENT:

You may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 378-4400
<http://www.doj.state.or.us/>

IF YOU ARE A RHODE ISLAND RESIDENT:

You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at:

RI Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
<http://www.riag.ri.gov/>

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account

relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.