BakerHostetler

Baker&Hostetler LLP

811 Main Street
Suite 1100
Houston, TX 77002-6111

T 713.751.1600
F 713.751.1717
www.bakerlaw.com

William R. Daugherty
direct dial: 713.646.1321
wdaugherty@bakerlaw.com

April 20, 2018

VIA EMAIL (SECURITYBREACH@ATG.WA.GOV) AND OVERNIGHT MAIL

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Attorney General Ferguson:

We are writing on behalf of our client, Southwest Airlines Co. ("Southwest"), to notify you of a security incident involving Washington residents.

On March 22, 2018, Southwest was informed by its former, third-party vendor, Orbitz LLC ("Orbitz"), that certain hotel reservations made through Orbitz and certain of its business partners' websites powered by Orbitz, including www.Southwest.com, may have been affected in a security incident involving a legacy Orbitz travel booking platform (the "Orbitz platform"). Upon learning this, Southwest immediately commenced an investigation and began working with Orbitz to determine the scope and nature of the incident. According to Orbitz, while conducting an investigation of Orbitz's platform, Orbitz determined on March 1, 2018 that there was evidence suggesting that, between October 1, 2017 and December 22, 2017, an unauthorized third-party may have accessed certain personal information stored on the Orbitz platform relating to reservations made through Orbitz and certain of its business partners' websites powered by Orbitz. The personal information that was likely accessed may have included individuals' names, payment card numbers and expiration dates, phone numbers, email addresses, and physical and/or billing addresses. This incident did not affect Southwest Airlines systems nor other travel reservations made through Southwest.com.

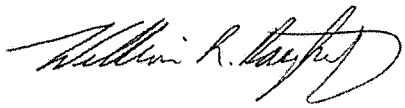
Today, Orbitz, working with Southwest, will begin notifying five hundred and fifty-five (555) Washington residents via U.S. mail in accordance with Wash. Rev. Code § 19.255.010 in

substantially the same form as the enclosed letter. Orbitz is offering eligible individuals one year of complimentary credit monitoring and identity protection services. Orbitz has also provided a telephone number for potentially affected individuals to call with any questions they may have.

To help prevent a similar incident from happening in the future, Orbitz took immediate steps to investigate the incident and enhance security and monitoring of the affected platform, and remediate the issue, including taking action to eliminate and prevent unauthorized access to the platform.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



William R. Daugherty
Partner

Enclosure

ORBITZ

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

07580
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

April 20, 2018

NOTICE OF DATA INCIDENT

Dear John Sample:

Orbitz is writing to make you aware of a data security incident affecting a legacy Orbitz travel booking platform (the "Orbitz platform") that powered our, and a number of our business partners', travel sites. Regrettably, certain hotel reservations that you made through Southwest.com, which was powered by Orbitz, may have been affected. This notice describes the incident, the measures taken in response, and some steps you can take to further protect your information.

What Happened?

While conducting an investigation of the Orbitz platform, Orbitz determined on March 1, 2018 there was evidence suggesting that, between October 1, 2017 and December 22, 2017, an unauthorized third-party 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 Orbitz platform and made every effort to remediate the issue, including taking swift action to eliminate and prevent additional unauthorized access to the platform.

Findings from our investigation indicate that the information accessed on the Orbitz platform included certain hotel reservations made through Southwest.com, and powered by Orbitz, during the period from January 1, 2016 to June 23, 2016. To date, we do not have direct evidence that this personal information was actually taken from the Orbitz platform. This incident did not affect Southwest Airlines' systems nor other travel reservations made through Southwest.com.

What Information Was Involved?

Orbitz determined that the personal information likely accessed may have included your name, payment card number and expiration date, phone number, email address, and physical and/or billing address.

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. Orbitz also began working with law enforcement and took measures to effectively prevent any additional 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.

Additionally, Orbitz is offering you 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 on the following pages.

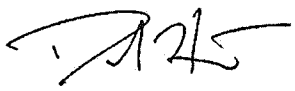
What You Can Do

Regardless of whether you elect to enroll in the credit monitoring and identity protection service, we recommend that you remain vigilant by reviewing your payment card account statements for any unauthorized activity. You should immediately report any unauthorized charges to your bank or other card issuer because the bank or other card issuer will generally reimburse fraudulent charges that are reported in a timely manner. Please also see the "Additional Steps You Take" section included on the following pages for additional information on ways to protect your information.

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/*.

Sincerely,



Daniel Hest
SVP & General Manager, Expedia Global Partner Solutions

ALLCLEAR ID IDENTITY PROTECTION SERVICE

For affected U.S. customers, the following services are available for 12 months after enrollment:

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: 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.

ADDITIONAL STEPS YOU CAN TAKE

Even if you choose not to take advantage of this complimentary credit monitoring, we remind you to remain 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. You may also want to 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:

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

If you are a resident of Connecticut, Maryland, or North Carolina, you may contact and obtain information from your state attorney general at:

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us,
1-888-743-0023 (toll free when calling within Maryland)
(410) 576-6300 (for calls originating outside Maryland)

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three (3) major reporting agencies by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

In order to request a security freeze, you will need to provide the following information:

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, provide 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, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.