May 3, 2018

To: U.S. State Attorney General and Consumer Protection Offices Distribution List

Re: Notice of Data Breach

Dear Sir or Madam,

We take data security seriously here at Alaska Airlines, and we value the trust our customers put in us to protect their information. I am writing to inform you of a recent matter involving Alaska's third-party service provider Orbitz, which did not meet our expectations and may have affected the personal information of individuals who are resident in your state (see Exhibit A).

As was reported in the news, Orbitz had a data security incident that affected an older Orbitz website and legacy platform. On March 19, 2018, Orbitz notified Alaska that Orbitz of this data security incident. Between October 1, 2017 and December 22, 2017, personal data on a legacy Orbitz platform relating to hotel or car reservations made via a white label Alaska website may have been accessed. The data potentially accessed includes name, date of birth, phone number, email address, physical/billing address, gender, and credit card information for reservations made between January 1, 2016 and December 5, 2016. Importantly, this matter does not involve any malware or security issues associated with Alaska's systems. Rather, information on this legacy Orbitz platform may have been affected by a breach to Orbitz' security.

Since being notified by Orbitz, Alaska has been working to understand the impact and any further steps that can be taken to assist affected customers. Alaska has been in regular communication with Orbitz regarding this matter and has been assured that unauthorized access in this manner to this legacy portal has been halted as of December 22, 2017.

All affected individuals are eligible, without enrollment, for identity theft repair services. Additionally, affected individuals can enroll in 12 months of complimentary credit monitoring and fraud alerts. Information about these offerings, provided by AllClear ID, is contained in the separately attached template notification letter, which we plan to send to all potentially affected individuals this week.

If you have any questions, please do not hesitate to call me at (206) 392-5234 or email me at Holly.Gion@alaskaair.com.

Respectfully submitted,

Holly Gion
Director, Data Privacy

Attachments

Exhibit A

Approximate number of potentially affected residents in Washington: 1,442

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

00001
ACD1234

00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

NOTICE OF DATA BREACH

May 4, 2018

Dear John Sample,

In 2016, you reserved a hotel or car through our website, which was powered at the time on the backend by an Orbitz platform. Orbitz recently notified us that there was a data security incident involving your transaction information that resulted in unauthorized access to some of your personal data. The details are below, but I would like to begin with an apology. We take data security seriously here at Alaska, and we value the trust you put in us to protect your information. In this case, our partner at the time, Orbitz, did not meet our expectations for data security. Please read below to learn more about what happened and what you can do.

WHAT HAPPENED?

Alaska partnered with Orbitz to provide the ability for our guests to make hotel and car reservations. According to Orbitz, a breach impacted transactions made on their platform between January 1, 2016 and December 5, 2016. Specifically, an unauthorized third party appears to have accessed personal information related to those transactions between October 1, 2017 and December 22, 2017.

WHAT INFORMATION WAS INVOLVED?

Personal data including your name, date of birth, phone number, email address, physical/billing address, gender, and credit card information may have potentially been involved. Passport information and travel itineraries were not exposed. Social security numbers were never collected, and therefore not impacted.

WHAT WE ARE DOING.

Orbitz notified us of the incident on March 19, 2018, and since then, we've been working to understand the impact and any further steps that can be taken to assist affected customers. Orbitz has advised that it is working to improve security on the platform. We understand this is not the service you expect when working with us or our travel partners, and we share that feeling. Our data security practices include a continued investment in staffing, systems, and tools to help protect your data. We utilize highly trained staff, automated scanning tools, and monitoring software that searches for malicious activity, security weaknesses, and unauthorized access. Although we stopped using the affected platform in 2016, we recommend you follow the below next steps.

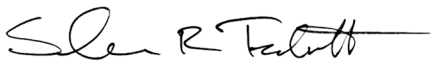
WHAT YOU CAN DO.

1) We encourage you to enroll in a free year of credit monitoring and identity protection service being offered to you by Orbitz. Instructions are in **Attachment A**.
2) We urge you to remain vigilant against threats of identity theft or fraud, and by regularly reviewing your account statements and monitoring your account statements and credit history for any signs of unauthorized transactions or activity.
3) If you suspect you are the victim of identity theft or fraud, you have the right to file a report with the police or law enforcement. In addition, you may contact the FCC or your State Attorney General to learn about the steps you can take to protect yourself against identity theft. **Attachment B** contains more information about steps you can take to protect yourself against fraud and identity theft.
4) Be alert for "phishing" emails by someone who acts like they know you and requests sensitive information over email, such as passwords, Social Security numbers, or bank account information. We do not ask for this type of sensitive information over email.

OTHER IMPORTANT INFORMATION.

If you have any questions about this letter 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 at 1-800-252-7522 (1-800-ALASKAAIR).

Sincerely,



Shane Tackett
Senior Vice President, Revenue and E-commerce
19300 International Blvd, Seattle, WA 98188

Attachments

ATTACHMENT A

Enrollment Information for Complimentary Credit Monitoring and Identity Protection

For affected U.S. customers, 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 1-855-828-5646 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 requires enrollment. It 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.

ATTACHMENT B

Additional Information Regarding Fraud and Identity Theft

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, security 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, SECURITY FREEZE, OR CREDIT LOCK

To place a fraud alert, security 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 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.

Security Freeze: Certain U.S. state laws, including in Massachusetts, provide the right to place a security freeze on your credit file. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a security 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 security 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 security freeze, you will be provided a PIN to lift temporarily or remove the security freeze. A security freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years. The cost to place a security 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 security freeze.

Credit Lock: Like a security freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike security 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, security 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.

U.S. Federal Trade Commission (FTC): The FTC has information about how to avoid identity theft and other steps that consumers can take to protect themselves. Write to: Consumer Response Center, 600 Pennsylvania Ave., NW, H-130, Washington, D.C. 20580; Call Toll-Free: 1-877-IDTHEFT (438-4338); or http://www.ftc.gov/idtheft.

Iowa Residents: You may contact local law enforcement or the Iowa Attorney General's Office at 1305 E. Walnut St., Des Moines, IA 50319; Tel: (515) 281-5164; or http://www.iowa.gov/government/ag.

Maryland Residents: You may obtain information about preventing identity theft from the FTC or the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202; Tel: (888) 743-0023; or http://www.oag.state.md.us.

New Mexico Residents: You have a right to place a security freeze on your credit report or submit a declaration of removal with a consumer reporting agency pursuant to the Fair Credit Reporting and Identity Security Act (FCRA). 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.

North Carolina Residents: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699-9001; Tel: (919) 716-6400; Fax: (919) 716-6750; or http://www.ncdoj.com.

Rhode Island Residents: You may obtain information about preventing identity theft from the FTC or the Rhode Island Attorney General's Office at 150 South Main Street, Providence, RI 02903; Tel: (401) 274-4400; or http://www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.