ORBITZ

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

00001
ACD1234

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.

American Express Company
200 Vesey Street
New York, NY 10285-0106

March 16, 2018

JOHN DOE
American Express AEDR
18850 N 56th Street
PHOENIX AZ
85032

American Express® Card Account ending in: 00111

RE: NOTICE OF DATA BREACH (ORBITZ)

Dear JOHN DOE,

Protecting the security of our Card Members' information is very important to us and we strive to let you know about security concerns as soon as possible. This letter describes unauthorized access to certain personal information that may have occurred at Orbitz, a third party vendor used by Amextravel.com and Amex Travel Representatives.

WHAT HAPPENED?
On March 16, 2018, Orbitz alerted us that it was the victim of a cyber attack. The attack involved Orbitz customers and customers of their business partners, and occurred on a platform that serves as the underlying booking engine for Amextravel.com and travel booked through Amex Travel Representatives. Certain transactions made on the Orbitz platform from January 1, 2016 through December 22, 2017 may have been impacted. Orbitz has assured us that its platform has been remediated. To be clear, this was an attack on the Orbitz platform. It was not an attack on, and did not compromise, the platforms American Express uses to manage your American Express® Card accounts.

WHAT INFORMATION WAS INVOLVED?
Orbitz has informed us that the personal information that may be at risk includes full name, payment card information, date of birth, phone number, email address, physical and/or billing address and gender. Orbitz has advised us that there is no evidence of unauthorized access to passport or travel itinerary information. Additionally, Social Security numbers were not involved in this incident, as these are neither collected nor held on the platform.

WHAT WE ARE DOING
We want to assure you that we are vigilantly monitoring your American Express Card account for fraud and, if it should occur, you are not liable for fraudulent charges on your account. To learn more about the measures we take to help protect your account visit our Security Center at **americanexpress.com/fraudprotection**.

We have also arranged for you to receive a complimentary two-year membership of Experian's IdentityWorks℠, which helps detect misuse of your personal information and provides you with identity protection focused on immediate identification and resolution of identity theft. In addition, if you believe there was fraudulent use of your information an Experian Identity Resolution agent is available to work with you to investigate and resolve each incident of fraud that occurred. The Terms and Conditions for this offer are located at **www.ExperianIDWorks.com/restoration**. You will also find self-help tips and information about identity protection at this site.

You will only receive the IdentityWorks benefits if you activate your membership. You can enroll online at **www.experianidworks.com/3bplusone** or by calling **1-877-890-9332**. If you choose to enroll in IdentityWorks via phone, you will need to provide the activation code and the engagement order number listed below. In addition, you will need to provide your Social Security number and a current U.S. mailing address to enroll.

Your personal IdentityWorks Activation Code: 58394BBB
Engagement Order Number: -84-052834-50
Enroll by: September 30, 2018 (your code will not work after this date)

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only*.
- **Credit Monitoring**: Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration**: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**: Provides coverage for certain costs and unauthorized electronic fund transfers**.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

WHAT YOU CAN DO

We ask that you carefully review your account for fraudulent activity. Below are some steps you can take to protect your account.

- **Login to your account at americanexpress.com/MYCA** to review your account statements carefully and remain vigilant in doing so, especially over the next 12 to 24 months.
- **If your card is active, sign up to receive instant notifications** of potential suspicious activity by enabling Notifications in the American Express Mobile app, or signing up for email or text messaging at **americanexpress.com/accountalerts**. Please make sure your mobile phone number and email address are also on file for us to contact you if needed.

OTHER IMPORTANT INFORMATION

Included with this letter are some additional helpful tips and steps you can take to protect yourself against the risks of fraud and identity theft. You may receive additional letters from us if more than one of your American Express Card accounts were involved.

FOR MORE INFORMATION

Please don't hesitate to call us 24 hours a day, 7 days a week, at **1-855-693-2213** – we are happy to assist you. As always, thank you for your trust in us, and for your continued Card Membership.

Especially in today's environment, we understand that your security is paramount. We are strongly committed to protecting the privacy and security of your information and regret any concern this may have caused you.

Sincerely,

Louise Thorpe
Chief Privacy Officer
American Express Company

Additional Helpful Tips

Below are additional helpful tips you may want to consider to protect your Card and personal information:

- **Login to your account at americanexpress.com/MYCA** to review your account statements carefully and remain vigilant in doing so, especially over the next 12 to 24 months.
- **If your card is active, sign up to receive instant notifications** of potential suspicious activity by enabling Notifications in the American Express Mobile app, or signing up for email or text messaging at **americanexpress.com/accountalerts.** Please make sure your mobile phone number and email address are also on file for us to contact you if needed.
- **Visit our Security Center at americanexpress.com/fraudprotection** to learn more about the measures we take to help protect your account and the steps you can take to safeguard your information.
- **Visit the Federal Trade Commission (FTC)** website for information on how to protect yourself against ID theft and safeguarding your electronic devices from viruses and other malicious software by:
  - *Learning how to make protecting yourself from identity thieves part of your daily routine by visiting **ftc.gov/idtheft** or call **1-877-IDTHEFT (438-4338)** to learn more about identity theft and protective steps you can take or file a report. You can also contact the FTC at: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington DC 20580.*
  - *Help avoid, detect and remove viruses and other malicious software by protecting your computer from spyware and viruses that can cause it to run slowly or give fraudsters access to your personal information by visiting **consumer.ftc.gov/articles/0011-malware**.*
- **Review this additional information:**
  - ***Maryland, North Carolina and Rhode Island** residents may also contact these agencies for information on how to prevent or avoid identity theft.*
    - ***For Maryland residents:** You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov/, 1-888-743-0023.*
    - ***For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Mail Service Center 9001, Raleigh, NC 27699-9001, http://www.ncdoj.gov/, 1-877-566-7226.*
    - ***For Rhode Island residents:** You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.*
  - ***For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.*
  - ***For Massachusetts residents:** You have the right to obtain a police report regarding this 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.*
  - ***For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.*
  - ***For Rhode Island residents:** You have the right to file or obtain a police report regarding this incident.*
- **Contact the major credit bureaus** to get useful information about protecting your credit, including information about fraud alerts, security freezes, or other steps you can take to protect yourself from fraud and identity theft. To obtain an annual free copy of your credit reports, visit **annualcreditreport.com**, call toll-free at 1-877-322-8228. Credit bureau contact details are provided below:

Equifax:	**Experian:**	**TransUnion:**
equifax.com	**experian.com**	**transunion.com**
freeze.equifax.com	**experian.com/freeze**	**transunion.com/freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834
1-800-525-6285	1-888-397-3742	1-800-916-8800

- ***For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:*** *You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).*
- *A fraud alert indicates to any business requesting your credit file that you suspect you are a victim of fraud and requires the business to verify your identity before issuing you credit. A fraud alert does not affect your ability to get a loan or credit, but it may cause some delay if you are applying for credit.*
- *A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a security freeze may delay your ability to obtain credit. To place a security freeze, you must send a written request to each of the three credit bureaus listed above and provide the following information: (1) your full name; (2) SSN; (3) date of birth; (4) the addresses where you have lived over the past 5 years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; (7) if you are the victim of identity theft, the police report, investigative report, or complaint to a law enforcement agency; and (8) if you are not the victim of identity theft, payment by check, money order, or credit card. If you are not a victim of identity theft, the credit reporting agencies will charge you a fee for each security freeze.*
- ***For Massachusetts and Rhode Island residents:*** *The credit bureaus may require you to pay a fee to place, lift, or remove the security freeze. For Massachusetts residents, such fee may be up to $5.*

- **Obtain or file a police report** - You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.
- **Keep a record of your contacts** - Start a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

RBC Royal Bank®

March 21, 2018

To our valued client:

Recently, Orbitz issued an advisory regarding a data security incident which affected some of their partners and customers. Orbitz managed the RBC travel rewards platform prior to transitioning to our new travel website earlier this year. This incident does not impact the new travel website or RBC's own systems.

The enclosed letter from Orbitz details information about the incident and resources that are being offered to protect your personal information.

As a valued RBC client, please be assured that you are protected by RBC's Zero Liability Guarantee so you will not be held liable for any unauthorized transactions on your RBC credit card resulting from this incident. Also, as an Online Banking client, you can monitor your credit reports using our free CreditView Dashboard, which helps you check your credit score regularly with no negative impacts. We encourage you to regularly monitor your accounts and contact us immediately should you notice any unusual or unauthorized activity. If you have any questions about your accounts, please contact us at 1-877-777-2239.

We appreciate your business and remain committed to the protection of your information.

Sincerely,

Athena Varmazis
Senior Vice President, Credit Cards
RBC Royal Bank

ORBITZ

NOTICE OF DATA BREACH

We are writing to share important information about an Orbitz 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?

On March 1, 2018, while conducting an investigation of a data security incident affecting a legacy Orbitz travel booking platform (the "platform"), we determined that, between January 1, 2016 and December 22, 2017 there may have been unauthorized access to certain personal information . We immediately began investigating the incident 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?

The investigation indicates that there likely was unauthorized access to personal information. Specifically, full name, address, telephone number, and incomplete payment card information.

What Information was *Not* Involved?

Our investigation to date has not found any evidence of unauthorized access to other types of personal information. We can assure you that bank account information, payment card details (CVV number on the back of your card), Social Insurance Numbers, Social Security Numbers, passport and travel itinerary information were not accessed or involved in this incident.

What We Are Doing

We do and will continue to treat the security of all personal information as a top priority. We took immediate steps to investigate the incident using a leading cybersecurity firm, notified law enforcement and payment card partners about the incident, and enhanced security and monitoring of the affected Platform.

RBC also immediately put into place enhanced credit card monitoring to help ensure you would not be affected by this incident further. You are also protected by RBC's Zero Liability Guarantee so you will not be held liable for any unauthorized transactions on your RBC credit card that result from this incident.

What You Can Do

In addition to the services mentioned above, we recommend that you remain vigilant in regularly reviewing and monitoring your account statements and credit history. If you are an Online Banking client with RBC, you can use their free CreditView Dashboard tool to monitor your credit reports with no negative impact to your credit score.

If you suspect that your payment card has been misused, please contact your financial institution [or call the number on the back of your card]. For RBC-issued payment cards, please contact RBC at 1-877-777-2239. **Attachment A** 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.

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.

ORBITZ

ATTACHMENT A

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 (Toll-free U.S.) or 1-512-201-2217 (International) 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 (Toll-free U.S.) or 1-512-201-2217 (International).

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.

ORBITZ

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.

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.

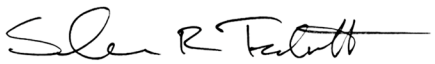
WHAT YOU CAN DO.

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.