American Express Company
General Counsel's Office
200 Vesey Street
New York, NY 10285

March 22, 2018

BY U.S. MAIL

Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

On behalf of American Express Travel Related Services Company, Inc., and pursuant to N.H. Rev. Stat. § 359-C:20(I)(b), this letter provides notice of a computer data security incident. The incident occurred at Orbitz, a third party vendor to American Express. An Orbitz platform provides the booking engine for reservations made online through Amextravel.com, and for reservations made by telephone through American Express Travel Representatives.

On March 16, 2018, Orbitz advised us of the following facts:

- The Orbitz platform that supports Amextravel.com and the telephone booking service was the victim of an external cyber attack in 2017.

- For transactions made on the Orbitz platform from January 1, 2016 through December 22, 2017, there may have been unauthorized access to certain personal information of American Express travel customers using Amextravel.com or making reservations through American Express Travel Representatives – specifically, name, card type, card number and expiration date, as well as date of birth, phone number, email address, physical and/or billing address, and gender.

- There is no direct evidence that this personal information was actually taken from the Orbitz platform.

- There is no evidence of unauthorized access to card security codes or passport or travel itinerary information.

- Based upon the information we have currently, it appears that the number of potentially impacted American Express Card Members in New Hampshire – i.e., Card Members with physical addresses in New Hampshire who made travel bookings through Amextravel.com or our telephone booking service between January 1, 2016 and December 22, 2017 – is 1,346.

- Since learning of the incident, Orbitz has remediated its platform.

Social Security numbers were not involved in this incident, as these are neither collected nor held on the Orbitz platform.

We are working with Orbitz to further understand this incident. Our ongoing efforts may change our understanding of the facts. If we learn material additional facts, we will provide an update.

To be clear, this incident did not occur on or compromise American Express's own systems. In particular, this was not an attack on, and did not compromise, the platforms that American Express uses to manage American Express Card accounts.

American Express is in the process of notifying our affected travel customers. A sample of the letter is enclosed. Mailing of these notices is in process, and is expected to be completed on or about March 23, 2018. As stated in the attached sample notice, American Express is offering to provide affected customers with two years of free credit monitoring services and identity theft protection services.

American Express takes this incident seriously, and is committed to answering any questions that your office may have about it. Please do not hesitate to contact me at 212-640-5051 or Sarah.E.Statz@aexp.com.

Respectfully yours,

Sarah E Statz

Sarah E. Statz
Vice President and Senior Counsel
200 Vesey Street
New York, NY 10285
Sarah.E.Statz@aexp.com

Enclosures

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 memberhip. 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.