

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

Date:

Card Member Name
Street Address
City, State, Zip Code

American Express® Card Account ending in: X-XXXX

RE: NOTICE OF DATA BREACH

Dear [Name],

WHAT HAPPENED?

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. We have been informed that during the course of an ongoing investigation, law enforcement officials recovered illegally obtained personal and account information. Account information of some of our Card Members, including some of your account information, may have been included among the data recovered by law enforcement. It is important to note that American Express owned or controlled systems were not compromised by this incident, and we are providing this notice to you as a precautionary measure.

WHAT INFORMATION WAS INVOLVED?

At this time, we have been informed that your current or previously issued American Express Card account number, your name and other Card information such as the expiration date, may have been compromised. The exact information recovered by law enforcement is not available at this time. Please be aware that you may receive additional letters from us if more than one of your American Express Card accounts were involved.

WHAT WE ARE DOING.

Please be assured we are vigilantly monitoring your 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.

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.

FOR MORE INFORMATION.

If you notice any suspicious activity on your account, please don't hesitate to call us 24 hours a day, 7 days a week, at **1-855-693-2213**. One of our Customer Care Professionals will be happy to assist you.

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. As always, thank you for your trust in us, and for your continued Card Membership.

Sincerely,

Anneke Covell
Vice President, U.S. & AENB Privacy
American Express Company

Additional Helpful Tips

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

- If your card is active, 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 consumer.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, or call toll-free at 1-877-322-8228. Credit bureau contact details are provided below:

Equifax:
equifax.com

Experian:
experian.com

TransUnion:
transunion.com

freeze.equifax.com
P.O. Box 105788
Atlanta, GA 30348
1-800-525-6285

experian.com/freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

transunion.com/freeze
P.O. Box 2000
Chester, PA 19016
1-888-909-8872

- *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.
- You have the right to place a security freeze on your credit file free of charge. 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 contact 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 2 years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze. There is no fee to place or lift a security freeze.
- **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.
- *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.
- You have the right to place a security freeze on your credit file free of charge. 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 contact 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 2 years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to

place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze. There is no fee to place or lift a security freeze.

- **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.