

American Express
200 Vesey Street
New York, NY 10285



[Insert date]

<CM Name>
< Address Line 1 >
<Address Line 2>
<City>, < State> <ZipCode>
<Country>

American Express® Card Account ending in: [LastFiveDigits]

RE: NOTICE OF THIRD-PARTY SECURITY INCIDENT

Dear [First_Name],

Protecting our customer information is a priority at American Express and we strive to let you know about security concerns as soon as possible. We've learned that one of our service providers had an incident that may have impacted some information related to you and your American Express account.

WHAT HAPPENED

On July 26, 2022, we were notified by an American Express third-party service provider that it had been the victim of a cyber attack and on November 3, 2022 we confirmed some of your information was impacted. We can assure you that this incident was not an attack on, nor did it compromise, any American Express systems.

WHAT INFORMATION WAS INVOLVED

The information that was compromised includes [insert data elements].

WHAT WE ARE DOING

We are actively monitoring your account for any signs of fraud. If we identify fraudulent activity on your account, we will take measures to protect your account and may contact you. You will not be held liable for any fraudulent charges. In addition, we are working closely with the third party to learn more about this incident.

WE'RE PROVIDING ADDED PROTECTION

We're pleased to offer you a complimentary two-year membership with Experian IdentityWorksSM, which helps detect misuse of your personal information and provides you with identity-theft protection services. Here's how it works:

Experian monitors your accounts to identify fraud or theft. It also provides fraud resolution assistance. If fraud is detected, an Experian Identity Resolution agent will investigate the matter and work to resolve the incident.

To receive your free benefits, you will need to activate your membership with Experian by enrolling online at experianidworks.com/3bplus or by calling 1-877-890-9332. To enroll, you'll need to provide the activation code below, your Social Security number, and a current U.S. mailing address. If you enroll via phone, you'll also need to provide the below engagement order number:

Personal Identity Works Activation Code: [RRRRRRRRR]

Engagement Order Number: [RRRRRRR]

Enroll by: [date] (your code will not work after this date)

Already have an Experian IdentityWorks membership? You can use the credentials above to extend your coverage for two years from the date you activate, free of charge.

Once you enroll in Experian IdentityWorks, you'll have complimentary access to:

- **Experian Credit Report:** Details on the information associated with your credit file. Daily credit reports are available for online members only*.
- **Credit Monitoring:** Active monitoring of your Experian, Equifax, and Transunion files for indicators of fraud.
- **Internet Surveillance:** 24/7 scans across the internet to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Immediate access to Identity Restoration specialists to help address and resolve credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** The same exceptional level of Identity Restoration support is available even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance:** Coverage for certain costs and unauthorized electronic fund transfers resulting from a case of identity theft**.

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

**The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Want more information? You can find the terms and conditions of this offer, along with tips for safeguarding your identity, at experianidworks.com/restoration.

WHAT YOU CAN DO

We recommend regularly monitoring your account for fraudulent activity. If you detect or suspect fraudulent activity on your account, contact us as soon as possible to report any suspicious activity or suspected identify theft.

Additionally, here are a few ways you can proactively protect your account:

- Log in to your account online at americanexpress.com/MYCA to review your account statements. We suggest checking your statements regularly and vigilantly over the next 12 to 24 months.
- Log into your Amex® App to activate free Card fraud and account activity alerts by enabling notifications. You can also sign up for email or text alerts at americanexpress.com/accountalerts. Make sure your personal information is updated on your account with your current email address and phone number so that we can contact you as needed.
- Visit our Security Center at americanexpress.com/us/security-center for more information on how we work to protect your account and what you can do to safeguard your personal information.
- Take action to protect yourself against identity theft and safeguard your electronic devices from viruses and other malicious software.
 - *Learn more about how you can protect yourself from identity theft or file a report by visiting consumer.gov/idtheft or calling 1-877-IDTHEFT (438-4338). You can also contact the FTC by mail at: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington DC 20580.*
 - *Learn how to avoid, detect, and remove viruses and other malicious software from your electronic devices by visiting consumer.ftc.gov/articles/0011-malware.*
- Contact the three major credit bureaus (Equifax, Experian, and TransUnion) for information about protecting your credit, preventing identify theft, setting up fraud alerts, and activating security freezes. We encourage you to periodically obtain and review your credit report from each major credit bureau. If you identify information relating to fraudulent transactions on your credit report, immediately contact the relevant credit bureau to have the information deleted. Contact information for the credit bureaus is available in the **Additional Helpful Tips** sheet included with this letter.

OTHER IMPORTANT INFORMATION

If you have more than one account with us, we may reach out again if we find that another account of yours was impacted by this incident. Review the Additional Helpful Tips sheet that is included with this letter for more information on steps you can take to protect yourself against risks of fraud and identity theft.

FOR MORE INFORMATION

We're here for you. Feel free to give us a call at any time at 1-855-693-2213. Our Customer Care Professionals are ready to assist you 24/7.

We're strongly committed to protecting the security of your account and we're sorry for any inconvenience this incident may have caused.

Sincerely,

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

Additional Helpful Tips

Here are a few additional tips to protect your Card and personal information:

- For more information about protecting your credit, you can contact the three major credit bureaus (Equifax, Experian, and TransUnion) for information about protecting your credit, preventing identify theft, setting up fraud alerts¹, and activating security freezes². We encourage you to periodically obtain and review your credit report from each major credit bureau. If you identify information relating to fraudulent transactions on your credit report, immediately contact the relevant credit bureau to have the information deleted.

Equifax: equifax.com freeze.equifax.com P.O. Box 105788 Atlanta, GA 30348 1-800-525-6285	Experian: experian.com experian.com/freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742	TransUnion: transunion.com transunion.com/freeze P.O. Box 2000 Chester, PA 19016 1-888-909-8872
--	---	---

¹A 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.

²You 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) Social Security Number; (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.

- Request or file a police report: You have the right to request any police report filed regarding 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: It is helpful to maintain a file with copies of your credit reports, any existing police reports, relevant correspondence, and copies of

disputed bills. It is also useful to maintain a log of your conversations with creditors, law enforcement officials, and any 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).
- **Maryland, North Carolina, and Rhode Island residents** may also contact the following agencies for information on how to prevent or avoid identity theft:
 - **For Maryland residents:** Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, marylandattorneygeneral.gov/, 1-888-743-0023.
 - **For North Carolina residents:** The North Carolina Office of the Attorney General, Mail Service Center 9001, Raleigh, NC 27699-9001, ncdoj.gov/, 1-877-566-7226.
 - **For Rhode Island residents:** The Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, 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.