



NATIONAL RAILROAD PASSENGER CORPORATION
1 Massachusetts Ave NW, Washington, DC 20001

December 26, 2024

Via E-mail (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

In accordance with Md. Code Ann., Com. Law § 14-3504, I am writing on behalf of the National Railroad Passenger Corporation ("Amtrak" or the "Company") to notify you regarding the nature and circumstances of a recent data security issue.

Amtrak recently learned that an unauthorized party may have used the login credentials of certain Amtrak customers to gain access to fourteen (14) their Amtrak Guest Rewards accounts on or around October 18, 2024 to October 21, 2024. Of the accounts affected by the incident, approximately one (1) account belonged to a Maryland resident. The Company believes that the unauthorized party may have obtained the login credentials from third-party sources. Amtrak has not found any indication that the customers' login credentials were obtained from the Company's systems.

While logged into the customers' Amtrak Guest Rewards accounts, the unauthorized party may have accessed certain information available through the Amtrak Guest Rewards profiles such as names, contact information, Amtrak Guest Rewards account numbers, dates of birth, payment details (such as partial credit card numbers and expiration dates for any stored credit card), gift card information (such as card numbers and PINs) and information about customers' transactions and trips with the Company.

Promptly after becoming aware of the issue, Amtrak took steps to investigate and secure the affected customers' Amtrak Guest Rewards accounts, including initiating a reset of affected customers' account passwords and requiring multi-factor authentication on their accounts. The Company also notified law enforcement. Amtrak is notifying approximately 1 affected Maryland resident by email. Enclosed is a sample of the notice being sent to affected individuals.

Please do not hesitate to contact me if you have any questions.

Very truly yours,

A handwritten signature in dark ink, appearing to read "Will H. Hunt", with a stylized flourish at the end.



NATIONAL RAILROAD PASSENGER CORPORATION
1 Massachusetts Ave NW, Washington, DC 20001



December 20, 2024

RE: CUSTOMER ACCOUNT BREACH NOTIFICATION

Dear Valued Customer,

We are writing to provide you with information regarding a security issue involving your Amtrak Guest Rewards account.

What Happened?

We recently learned that an unauthorized party may have used your login credentials to gain access to your Amtrak Guest Rewards account between **October 18, 2024, and October 21, 2024**. We believe that the unauthorized party may have obtained your login credentials from third-party sources. We have no indication that your login credentials were obtained from our systems.

What Information Was Involved?

While logged into your Amtrak Guest Rewards account, the unauthorized party may have accessed certain information available through your Amtrak Guest Rewards profile such as your name, contact information, Amtrak Guest Rewards account number, date of birth, payment details (such as partial credit card numbers and expiration dates for any stored credit card), gift card information (such as card number and PIN) and/or information about your transactions and trips with us.

What We Are Doing

Promptly after becoming aware of the issue **on October 18, 2024**, we began an investigation and took steps to secure your account. We have initiated a reset of your account password and enabled multi-factor authentication for your account.

What You Can Do

We are alerting you about this issue so you can take steps to help protect your information, including:

- **Change Your Login Credentials.** When you reset your Amtrak Guest Rewards account password, use a unique password that is not easy to guess or used for other accounts. In addition to changing the password to your Amtrak Guest Rewards account, consider changing your credentials for other online accounts for which you use the same or a similar username and password and review those accounts for any suspicious activity.
- **Utilize Enabled Multifactor Authentication.** As a precaution to improve your account security and prevent unauthorized account access, Amtrak has enabled multifactor authentication on your Amtrak Guest Rewards account. Upon logging into your Amtrak Guest Rewards account, you will be offered a choice to receive a validation code either by email or text. After you receive the code, you enter it into the website or app to complete your login.
- **Review the Reference Guide.** The Reference Guide below provides recommendations by the U.S. Federal Trade Commission on the protection of personal information.



For More Information

We hope this information is useful to you. If you have any questions regarding this issue, please contact us at: **1-800-307-5000**

Sincerely,

Amtrak Guest Rewards Customer Care Team



Reference Guide

We encourage affected individuals to take the following steps:

Order Your Free Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228 or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. You should always remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your free credit reports. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/



Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC, as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)



(410) 576-6300

www.marylandattorneygeneral.gov

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
<https://ag.ny.gov/>

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
<https://ag.ny.gov/resources/individuals/consumer-issues/technology>

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)



(503) 378-4400
www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)-274-4400
www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202)-727-3400
www.oag.dc.gov



December 20, 2024

RE: **CUSTOMER ACCOUNT BREACH NOTIFICATION**

NOTICE OF DATA BREACH

Dear Valued Customer,

We are writing to provide you with information regarding a security issue involving your Amtrak Guest Rewards account.

What Happened?

We recently learned that an unauthorized party may have used your login credentials to gain access to your Amtrak Guest Rewards account between **October 18, 2024, and October 21, 2024**. We believe that the unauthorized party may have obtained your login credentials from third-party sources. We have no indication that your login credentials were obtained from our systems.

What Information Was Involved?

While logged into your Amtrak Guest Rewards account, the unauthorized party may accessed certain information available through your Amtrak Guest Rewards profile such as your name, contact information, Amtrak Guest Rewards account number, date of birth, payment details (such as partial credit card numbers and expiration dates for any stored credit card), gift card information (such as card number and PIN) and/or information about your transactions and trips with us.

What We Are Doing

Promptly after becoming aware of the issue **on October 18, 2024**, we began an investigation and took steps to secure your account. We have initiated a reset of your account password and enabled multi-factor authentication for your account.

What You Can Do

We are alerting you about this issue so you can take steps to help protect your information, including:

- **Change Your Login Credentials.** When you reset your Amtrak Guest Rewards account password, use a unique password that is not easy to guess or used for other accounts. In addition to changing the password to your Amtrak Guest Rewards account, consider changing your credentials for other online accounts for which you use the same or a similar username and password and review those accounts for any suspicious activity.
- **Utilize Enabled Multifactor Authentication.** As a precaution to improve your account security and prevent unauthorized account access, Amtrak has enabled multifactor



authentication on your Amtrak Guest Rewards account. Upon logging into your Amtrak Guest Rewards account, you will be offered a choice to receive a validation code either by email or text. After you receive the code, you enter it into the website or app to complete your login.

- Review the Reference Guide. The Reference Guide below provides recommendations by the U.S. Federal Trade Commission on the protection of personal information.

For More Information

We hope this information is useful to you. If you have any questions regarding this issue, please contact us at **1-800-307-5000**.

Sincerely,

Amtrak Guest Rewards Customer Care Team



Reference Guide

We encourage affected individuals to take the following steps:

Order Your Free Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228 or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. You should always remain vigilant for incidents of fraud and identity theft by reviewing your account statements and monitoring your free credit reports. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center



600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC, as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)



- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.marylandattorneygeneral.gov

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act (“FCRA”). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
<https://ag.ny.gov/>

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
<https://ag.ny.gov/resources/individuals/consumer-issues/technology>



For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)-274-4400
www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202)-727-3400
www.oag.dc.gov