



C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.myidcare.com/account-creation/protect>
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

June 9, 2020

Re: Notification of Data Security Incident

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident that may have involved some of your personal information. Pioneer Railcorp (“PRC”) takes the privacy and security of your information very seriously. This is why we are contacting you, offering you complimentary credit monitoring and identity theft restoration services, and informing you about steps you can take to help protect your personal information.

What Happened? On December 2, 2019, we discovered unusual activity in our email system. Upon discovering this activity, we immediately took steps to secure our digital environment and launched an internal investigation. We also engaged an independent forensics firm to determine what happened and whether personal information may have been accessed or acquired without authorization. We subsequently learned that certain employee email accounts of a PRC subsidiary had been accessed without authorization. Upon completion of the forensic investigation, we engaged a document review vendor to search the contents of the impacted email accounts to identify the individuals whose personal information may have been contained within those accounts. On May 1, 2020, we found that messages and/or attachments contained within the impacted email accounts included your personal information. While we are unaware of any evidence that anyone’s information has been misused as a result of this incident, we then worked diligently to identify up-to-date address information in order to notify all potentially impacted individuals. This process was completed on May 15, 2020.

What Information Was Involved? Based upon our investigation, the information may include your <<variable text>>.

What We Are Doing. As soon as we discovered the incident, we took the steps discussed above. In addition, we have taken affirmative action to minimize the likelihood of a similar incident occurring in the future. This includes working with leading cybersecurity experts to enhance the security of our digital environment and reporting the incident to the three major consumer reporting agencies. We also notified the FBI and will provide whatever cooperation is necessary to hold the wrongdoers accountable. Additionally, we are providing you with information about steps that you can take to help protect your personal information. As an added precaution, we are offering you complimentary MyIDCare™, identity theft protection services through ID Experts®, a data breach and recovery services expert. MyIDCare services twelve (12) months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services at no cost to you.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. Furthermore, while we do not believe anyone's information has been misused as a result of this incident, as a precautionary measure to safeguard your information, we encourage you to enroll in free MyIDCare services by calling 1-800-939-4170 or going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Please note that the deadline to enroll is September 9, 2020.

For More Information: We remain committed to protecting your personal information and apologize for any worry or inconvenience this may cause you. If you have any questions, please contact the ID Experts helpline at 1-800-939-4170 or go to <https://app.myidcare.com/account-creation/protect>, and have your unique code ready to provide to the fraud specialist.

Sincerely,

A handwritten signature in cursive script that reads "Carrie Genualdi".

Carrie Genualdi
Chief Financial Officer | Pioneer Railcorp

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.