Kennedys

1600 Market Street
Suite 1410
Philadelphia, PA 19103
USA

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 267 479 6795

Nicholas.Jajko@kennedyslaw.com

December 29, 2025

By Online Submission

Attorney General Mike Hilgers
Attn: Security Breach Notification
Nebraska Attorney General
2115 State Capitol
Lincoln, NE 68509

Re: Pacific Railway Enterprises – Notice of Data Incident

Dear Attorney General Hilgers:

We represent Pacific Railway Enterprises ("PRE"), a railroad system design and consulting firm located in Riverside, California. We write to notify your office of a data incident pursuant to Nebraska data breach notification statute Neb. Rev. Stat. § 87-803 impacting the personal information of six (6) Nebraska residents. In making this submission, PRE does not waive its rights or defenses regarding the applicability of Nebraska law or personal jurisdiction. This notice may be supplemented with new information learned after submission.

On November 13, 2025, PRE experienced a disruption to its computer network. PRE immediately took steps to secure its environment and partnered with professionals to investigate and understand the nature and scope of the disruption. On November 23, 2025, the investigation determined that certain files and folders were taken from PRE's network without authorization. PRE then began a comprehensive review of those files and folders to determine what sensitive information, if any, was contained therein and to whom it belonged. PRE completed its review on November 25, 2025, and is now notifying those individuals whose personal information was contained within the data set. The personal information included their names and Social Security numbers.

On December 29 2025, PRE provided written notice of the incident to potentially impacted individuals, including six (6) Nebraska residents via First Class U.S. mail. A sample copy of the notification letter is attached as Exhibit A.

PRE's notice of this incident includes a brief description of the incident and encouragement to remain vigilant for incidents of fraud or misuse, from any source, by reviewing account statements and credit reports. The notice also includes the recommendation to file a report with law enforcement, notify their state attorney general, and/or contact the Federal Trade Commission for more information. PRE confirmed the types of personal information subject to unauthorized access and enclosed contact information for the major consumer reporting bureaus, state-specific regulators, and the number for a dedicated call center for obtaining resources to protect against fraud or misuse, should the individual find it appropriate to do so. PRE is offering 12 months of single bureau credit monitoring, fraud consultation, and identity theft restoration services through Cyberscout, a TransUnion company, to the affected individuals.

Upon becoming aware of the incident, PRE immediately took steps to confirm the security of its environment and partnered with cyber incident response professionals to conduct an investigation into the nature and scope of the disruption. PRE also reported this incident to federal law enforcement. PRE is reviewing its existing security policies and protections previously in place on its network and adopting additional security to safeguard against evolving threats moving forward. PRE is reporting to other state regulators as required.

Should you have any further questions at this stage, please do not hesitate to contact me. Thank you.

Very truly yours,

/s/ Nicholas Jajko

Nicholas Jajko, Partner
Kennedys CMK, LLP

CC: Matthew Smith (Matthew.Smith@kennedyslaw.com)

Enclosures: Sample Consumer Notification Letter

Exhibit A

Pacific Railway Enterprises
c/o Cyberscout
PO Box 245
Bellmawr, NJ 08099

PACIFIC RAILWAY ENTERPRISES, INC.
3560 University Ave - Suite F - Riverside - CA 92501

[redacted]

December 29, 2025

NOTICE OF DATA BREACH

Dear [redacted]

Pacific Railway Enterprises ("PRE") takes the security and privacy of your personal information in our care very seriously. We write to inform you of an incident that involved your information. While we are unaware of any actual or attempted fraud or identity theft, we are providing you with information about the incident, our response, and steps you may take to better protect yourself, including the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On November 13, 2025, we experienced a disruption to our computer network. We immediately took steps to secure our environment and restore our operations safely. We partnered with professionals to investigate and understand the nature and scope of the disruption. On November 23, 2025, our investigation determined that certain files and folders were taken from our network without authorization. We then began a comprehensive review of those files and folders to determine what sensitive information, if any, was contained therein and to whom it belonged. We completed our review on November 25, 2025, and confirmed that certain personal information belonging to you was contained within the data set.

What Information Was Involved? The information involved included your name, [redacted] We reiterate that we have no indication of fraud or identity theft occurring as a result of this incident.

What We Are Doing. Upon becoming aware of this incident, we immediately took steps to confirm the security of our environment. We partnered with professionals to conduct an investigation into the nature and scope of the disruption and restore our operations safely. We reported this incident to federal law enforcement. We are also reviewing the existing security controls and policies & procedures we have in place to remain resilient against future threats.

In addition to providing you with notice of the incident, we are also offering you access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you discover suspicious activity. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Instructions for how to enroll are below.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, from any source, by reviewing your account statements, and monitoring your free credit reports for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or provider. Please refer to the enclosed *Steps You Can Take to Help Protect Your Information* which contains additional resources you may take advantage of, should you find it appropriate to do so.

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have any additional questions or concerns, please call our dedicated assistance line at 1-800-405-6108 Monday through Friday 5:00am – 5:00pm PT, excluding major U.S. holidays. Please know that the security of information is of the utmost importance to us. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Pacific Railway Enterprises Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts and Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To obtain a free annual credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Report Suspected Fraud. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, the state Attorney General, and the FTC.

Place Fraud Alert. You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Place Security Freeze. As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

To place a fraud alert or credit freeze, contact the three major credit reporting bureaus listed below:

TransUnion	**Experian**	**Equifax**
1- 800-916-8800	1-888-397-3742	1-888-378-4329
www.transunion.com	www.experian.com	www.equifax.com
TransUnion Fraud Alert	**Experian Fraud Alert**	**Equifax Fraud Alert**
P.O. Box 2000	P.O. Box 9554	P.O. Box 105069
Chester, PA 19016-2000	Allen, TX 75013	Atlanta, GA 30348-5069
TransUnion Credit Freeze	**Experian Credit Freeze**	**Equifax Credit Freeze**
P.O. Box 160	P.O. Box 9554	P.O. Box 105788

Woodlyn, PA 19094	Allen, TX 75013	Atlanta, GA 30348-5788

Obtain Additional Information. You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

Pacific Railway Enterprises, Inc. may be contacted by mail at 3560 University Ave, Suite F, Riverside, CA 92501. This notice has not been delayed by law enforcement.