



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Carolyn Purwin Ryan
Office: (267) 930-6836
Fax: (267) 930-4771
Email: CPurwinRyan@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 11, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Sierra Pacific Industries (“SPI”) located at 19794 Riverside Ave., Anderson, CA 96007, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SPI does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 11, 2022, SPI discovered its network was the target of a sophisticated cyberattack. SPI moved quickly to secure the network, then began an investigation to identify what happened and confirm what information may have been affected. Through its investigation, SPI determined that, between June 10, 2022, and June 11, 2022 an unauthorized actor may have had access to certain systems that stored personal information. SPI conducted a thorough and time-intensive review of the potentially accessible documents from these systems to determine what, if any, personal information may have been contained within them. Upon receiving the initial results of the review on November 23, 2022, SPI worked diligently to locate address information for those individuals whose information was present in the documents at the time of this event and completed that effort on December 30, 2022.

The information that could have been subject to unauthorized access includes name, Social Security number, medical information, and health insurance information.

Notice to Maryland Resident

On January 11, 2023, SPI provided written notice of this incident to one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, SPI moved quickly to investigate and respond to the incident, assess the security of SPI systems, and identify potentially affected individuals. Further, SPI notified federal law enforcement regarding the event. SPI is providing access to credit monitoring services for twelve (12) months, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, SPI is providing impacted individuals with guidance on how to better protect against identity theft and fraud. SPI is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

SPI is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-6836.

Very truly yours,

Carolyn Purwin Ryan of
MULLEN COUGHLIN LLC

CPR/kjc
Enclosure

EXHIBIT A



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF <<VAR DATA 3 – HEADER>>

Dear <<Name 1>>:

Sierra Pacific Industries (“SPI”) is writing to notify you of a recent incident that may affect the privacy of some of your information. Although we have no evidence of any identity theft or fraud occurring as a result of this incident, this letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On June 11, 2022, SPI discovered our network was the target of a sophisticated cyberattack. We moved quickly to secure the network, then began an investigation to identify what happened and confirm what information may have been affected. Through our investigation, we determined that, between June 10, 2022, and June 11, 2022, an unauthorized actor may have had access to certain systems that stored personal information. We conducted a thorough and time-intensive review of the potentially accessible documents from these systems to determine what, if any, personal information may have been contained within them. Upon receiving the initial results of the review on November 23, 2022, SPI worked diligently to locate address information for those individuals whose information was present in the documents at the time of this event and completed that effort on December 30, 2022.

What Information Was Involved? The investigation in this matter was unable to confirm whether information related to you was actually accessed or viewed by an unauthorized actor during this incident. However, SPI is notifying you out of an abundance of caution. The information related to you that was potentially accessible within the impacted files and folders includes your name and <<Breached Elements>>.

What We Are Doing. We take this incident and the security of information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of relevant SPI systems, and notify potentially affected individuals. Our response included resetting relevant account passwords, reviewing the contents of the potentially accessed files and folders to determine whether they contained sensitive information, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. We also notified and are cooperating with federal law enforcement. As part of our ongoing commitment to the security of information we are also reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

We are also offering you access to complimentary credit monitoring and identity protection services for <<Var Data 2 – CM Length>> months through TransUnion. These services include fraud consultation and identity theft restoration services. If you wish to activate the credit monitoring and identity protection services, you may follow the instructions included in the *Steps You Can Take to Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. You may also review the information contained in the attached *Steps You Can Take to Protect Personal Information*. There you will also find more information on the complimentary credit monitoring services we are making available to you. While SPI will cover the cost of these services, you will need to enroll yourself in the services we are offering, if you would like to do so.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-888-670-9832 between the hours of 6:00 a.m. and 6:00 p.m., Monday – Friday, except holidays. You may also write to SPI at P.O. Box 496028, Redding, California 96049.

We sincerely regret any inconvenience or concern this incident may have caused.

Sincerely,

A handwritten signature in black ink, appearing to read "Tony Jaegel", is positioned above the typed name and title.

Tony Jaegel
Vice President Human Resources
Sierra Pacific Industries

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for <<Var Data 2 – CM Length>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following 12-letter Activation Code <<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain <<Var Data 2 – CM Length>> months of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The subscription also includes access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, 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, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer’s 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 to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); 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.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.