



2049 Century Park East, Suite 2900 Los Angeles, CA 90067 • 310.229.1335

November 22, 2022

Pasha Sternberg
310.229.1335
415.276.4785 Direct Fax
psterberg@polsinelli.com

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General

Attn: Jeff Karberg, Administrator of the Identity Theft Program

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

Re: Notification of a Data Security Incident

Dear Mr. Karberg:

We represent Century Aluminum Company (“Century”) in connection with an incident that involved the personal information of Maryland residents and provide this notice on behalf of Century pursuant to MD. CODE ANN., COM. LAW § 14-3504(h). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Century is notifying you of this incident, Century does not waive any rights or defenses relating to the incident or this notice

NATURE OF THE INCIDENT

Century Aluminum Company (“Century”) learned that an unauthorized party gained access to its computer network. Upon discovering the situation, Century promptly began taking steps to contain it, and Century initiated an internal investigation. Century also engaged a forensic security firm, through legal counsel, to investigate and confirm the security of its systems. Through that investigation, Century learned that the unauthorized party had access to the Century network between January 28, 2022 and February 16, 2022 and may have had access to copies of some files in Century’s systems.

Based on these findings, Century undertook a comprehensive review of the files potentially accessed by the unauthorized party. On September 20, 2022, Century determined that these files contained some individuals’ personal information, including seven (7) residents of Maryland. The involved information varied by person but included one or more of the following: Social Security number, date of birth, health insurance information, and information regarding medical conditions, treatments or diagnoses. While Century has no evidence that anyone’s personal information has been misused, Century is notifying the individuals whose personal information was contained in the files potentially accessed by the unauthorized party.

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Washington, D.C. Wilmington
Polsinelli PC, Polsinelli LLP in California

86839535.1

November 22, 2022

Page 2

NOTIFICATION TO THE MARYLAND RESIDENTS

On November 17, 2022, Century mailed letters notifying the Maryland residents whose personal information was contained in the files potentially accessed by the unauthorized party. The notification letter includes an offer for complimentary credit monitoring and identity theft protection, as well as a telephone number that individuals can call if they have any questions regarding the incident. Enclosed is sample of the notice being sent via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, Century promptly contained it and began an internal investigation. Century engaged a forensic security firm to investigate and confirm the security of its computer systems. Century is undertaking efforts to reduce the risk of a similar incident occurring in the future, including reviewing its technical security measures. Finally, as discussed above, Century is notifying the potentially involved Maryland residents, providing them with information on how to protect against fraudulent activity and identity theft, and providing those whose Social Security numbers may have been accessed free credit monitoring services.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,



Pasha A. Sternberg

Enclosure

CenturyALUMINUM

Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-896-3993

Or Visit:

<https://response.idx.us/cac>

Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

November 17, 2022

Dear <<First>><<Middle>><<Last>><<Suffix>>:

RE: NOTICE OF DATA BREACH

Century Aluminum Company ("Century Aluminum" or "we") respects the privacy of our employees, former employees, business partners, and other individuals, and we are committed to keeping information entrusted to us confidential. Unfortunately, we are writing to advise you of a recent incident that may have involved some of your personal information. **We have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft.** Nonetheless, because your information was involved in the incident, we are providing you this notice with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? We recently learned that an unauthorized third party gained access to our computer network. Upon discovering the incident, we promptly began an internal investigation, and we engaged a leading computer forensics firm to further examine our network and confirm the security of our systems. Through that investigation, we learned that the unauthorized party had access to our network between January 28, 2022 and February 16, 2022 and acquired copies of some files in our systems.

What Information Was Involved? Upon identifying that the unauthorized third party may have acquired copies of some of our files, we began a review of the information in those files to determine what, if any, personal information may have been involved. On September 20, 2022, we determined that files contained your name, together with your <<Variable Text 1>>.

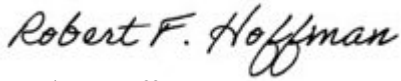
What We Are Doing. In addition to conducting an investigation into how the incident occurred, we are taking steps to reduce the risk of this type of incident occurring in the future, including implementing additional data security processes, new security software, and other technical controls. Additionally, although we have no evidence of information being used for the purposes of fraud or identity theft, we are offering identity theft protection services through IDX. IDX identity protection services include: 12 months of credit and CyberScan monitoring, an insurance reimbursement policy, and fully managed ID theft recovery services. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This product is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

What You Can Do. We encourage you to take advantage of the complimentary credit monitoring included in this letter. To enroll, call 1-833-896-3993 or go to <https://response.idx.us/cac> and use the Enrollment Code provided above. Please note the deadline to enroll is February 17, 2023. Additionally, if your username/email address and password were

involved as reported in the *What Information Was Involved* section above, we recommend you promptly change your password. You can also find more information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.

We understand that you may have questions that this letter does not answer. If you have questions, please call 1-833-896-3993 between 8 am – 8 pm Central Time, Monday through Friday.

Respectfully,

A handwritten signature in black ink that reads "Robert F. Hoffman". The signature is written in a cursive style with a large, stylized "H" and "F".

Robert Hoffman
Chief Information Officer

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring 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 should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, 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 a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected one (1) Rhode Island resident. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to 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.