



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

June 5, 2024

Bruce A. Radke
312-463-6211 Direct
312-819-1910 Fax
bradke@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 Potential Data Security Incident

Dear Mr. Karberg:

We represent Siemens Manufacturing Company, Inc. ("Siemens"), 410 W. Washington Street, Freeburg, Illinois 62243, in connection with an incident that may have involved the personal information of a single Maryland resident. Siemens is reporting the incident 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 this submission. While Siemens is notifying you of this incident, Siemens does not waive any rights or defenses relating to the incident.

NATURE OF THE INCIDENT

On March 26, 2024, Siemens observed evidence of suspicious activity on its network that resulted in the unauthorized encryption of its systems by an unknown third party. Upon discovering the incident, Siemens worked to isolate its network, move systems offline, and search for evidence of unauthorized activity. Siemens consulted with federal law enforcement and engaged with outside forensic experts to investigate the incident.

The investigation determined that the outside third party potentially acquired files from a limited portion of Siemens' network. Thereafter, Siemens worked to determine the contents of the compromised files. On April 26, 2024, Siemens' investigation determined that the personal information of a single Maryland resident was included in files potentially acquired by the third party. The files contained the individual's name and Social Security number. Siemens is not aware of any instances of identity fraud relating to the incident.

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

June 5, 2024

Page 2

NOTICE TO THE MARYLAND RESIDENT

Siemens notified the individual via physical mail yesterday, June 5, 2024. The notice includes a code to enroll in a twelve-month credit monitoring and identity theft protection service at no charge to the individual. A sample of the notice being provided to the Maryland resident is included in the materials accompanying this letter.

STEPS TAKEN RELATING TO THE INCIDENT

After discovering the incident, Siemens activated its incident response plan, which included taking steps to limit the exposure to information in its environment. Siemens notified state and federal law enforcement shortly after discovering the incident and worked in consultation with a team of independent cybersecurity and incident response professionals. As described above, Siemens is notifying the individual directly and is providing them with access to credit monitoring and identity theft protection services at no cost to them. Siemens is undertaking efforts to reduce the risk of a similar incident occurring in the future.

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.

Very truly yours,



Bruce A. Radke

Enclosures

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Dear <<Name>>:

Siemens Manufacturing Company values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information. This letter explains the incident, the steps we have taken in response, and provides information on steps you may take to help protect your information, should you feel it is appropriate to do so.

What Happened? On March 26, 2024, we discovered that an unauthorized third party gained temporary access to our network. Upon learning of the incident, we promptly took steps to contain and remediate the incident and began an internal investigation. We also notified law enforcement and engaged a forensic security firm to assist with our investigation and confirm the security of our computer systems. The forensic investigation determined that the unauthorized third party accessed some of our computer systems between March 21, 2024, until March 26, 2024, and may have accessed and acquired certain files from our systems during this period.

What Information Was Involved? We reviewed the contents of the relevant files for personal information and on April 26, 2024, it was determined that the files contained your name, date of birth, and Social Security number. We have no evidence that your personal information has been misused to date.

What We Are Doing. In addition to the actions described above, we are continuing to identify potential additional enhancements to our technical security measures. Although we are not aware of any instances of fraud or identity theft resulting from this incident, out of an abundance of caution, we are offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on prompt identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary, one-year membership, please see the additional information attached to this letter.**

What You Can Do. Again, while we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring included in this letter. You can also find more information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard personal information seriously, and apologize for any inconvenience this incident might cause. For further information and assistance, please call toll free at 888-327-0319 between of 8:00 a.m. to 8:00 p.m. CST, Monday through Friday excluding major holidays.

Sincerely,

Mike Siemens

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<Activation Code>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

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: By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report 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: By law, you have the right to place a fraud alert on your credit report if you believe you have been, or are about to become, a victim of fraud or related crime. 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/protectYourIdentity.action.

Credit and Security Freezes: By law, you 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 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
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
<https://www.experian.com/freeze/center.html>
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
<https://www.transunion.com/credit-freeze>
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 Mexico Residents: Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

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.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; <https://www.doj.state.or.us/>.

Rhode Island Residents: We believe that this incident affected <<RI>> Rhode Island residents. 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.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).