GT GreenbergTraurig

Kevin M. Scott
Tel 312.456.1040
Fax 312.456.8435
scottkev@gtlaw.com

May 19, 2021

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Via Email: attorneygeneral@doj.nh.gov

Re: Notification of Security Incident

Dear Attorney General Formella:

We write in furtherance of our previous correspondence dated January 26, 2021, concerning a data security incident impacting our client, the thyssenkrupp Materials group of companies in the United States and Canada ("tk Materials"). As previously advised, tk Materials suffered a ransomware attack on December 28, 2020. In an abundance of caution, tk Materials immediately notified certain current and former employees and family members whose information was contained on the affected server without regard to whether their information was at risk. Since that time, tk Materials has conducted an exhaustive search of approximately 150,000 documents to identify whether specific individuals' information was contained therein and to locate the affected individuals.

Beginning May 19, 2021, tk Materials, is notifying approximately 4 additional individuals for a total of 6 New Hampshire residents that their personal information may have been impacted in the security incident. Enclosed is a copy of the notification letter, in which tk Materials will also offer this population of individuals two years of triple bureau credit monitoring and identity theft protection services at no cost.

Please contact me for any additional information.

Best Regards,

Kevin M. Scott
Shareholder

thyssenkrupp

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 Data Breach

Dear <<Name 1>>:

What Happened?
On December 28, 2020, the thyssenkrupp Materials group of companies in the United States and Canada ("tk Materials") was the victim of a ransomware attack encrypting our servers and workstations. We took immediate action to investigate and isolate the attack and secure our IT environment. On January 28, 2020, we discovered certain electronic files had been compromised during that attack, and we have been working diligently to review, analyze, and sort through a significant volume of electronic files to identify personal data contained therein and to perform additional research necessary to locate affected individuals. On May 5, 2021, we completed our exhaustive review and analysis. We are sending this letter because your personal information was identified in our review as involved in that compromise.

What Information was Involved?
The threat actor obtained certain data in our system which included HR information about some of our current and former employees and certain of their family members or dependents. The information that may have been affected includes one or more of the following: name, address, social security number, birthdate, direct deposit information, payroll information, health information, and contact information.

What We are Doing
We take the security of personal information very seriously, and we want to assure you that we've already taken steps to prevent a reoccurrence by increasing the monitoring of our networks, further improving access controls and hardening our systems.

As we previously informed you in our prior communications, we have arranged for you to enroll, at no cost to you, in an online, three-bureau credit monitoring service (*my*TrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter 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, three-bureau 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 six-digit telephone [redacted] 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 **September 30, 2021**. 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. Enrolling in this service will not affect your credit score.

What You Can Do
Please review the enclosed "Additional Important Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC), regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file, should you choose to do so. You can also contact the FTC for more information.

As an added precaution, you may wish to monitor your personal accounts and change your passwords, particularly if you logged into any sensitive accounts (e.g., banking or financial institution accounts) from a tk Materials workstation. If you re-used your tk Materials account password(s) for any personal accounts, you should consider changing those passwords as well.

For More Information
If you have additional questions or concerns regarding this incident, please call 800-475-1420, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.

If you have questions regarding enrollment in the credit monitoring service, please call 1-855-288-5422, Monday through Friday from 9:00 a.m. to 7:00 p.m. Eastern Time. Please have your activation code ready.

PLEASE DO NOT CONTACT HR with questions. We have set up the toll-free numbers to answer any questions you may have about this incident and to assist you in enrolling in the complimentary services we are providing, should you need help.

We take the security of all information in our systems very seriously. Please know that the protection of your personal information is our utmost priority, and we sincerely regret any concern or inconvenience that this matter may cause you.

Sincerely,

Ellen Wood
VP Human Resources

Additional Important Information

For residents of *Iowa*: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *New Mexico:* You are advised to review your personal account statements and credit reports, as applicable, to detect errors resulting from the security incident, and your rights pursuant to the federal Fair Credit Reporting Act. Please see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

DC Attorney General
400 6th Street NW
Washington, D.C. 20001
1-202-727-3400
www.oag.dc.gov

Maryland Office of Attorney General
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of Attorney General
150 South Main Street
Providence, RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Attorney General
9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
www.ncdoj.com

New York Attorney General
120 Broadway
3rd FloorNew
York, NY 10271
www.ag.ny.gov

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.identitytheft.gov

For residents of *Massachusetts and Rhode Island*: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (https://www.experian.com/fraud/center.html), or Transunion (https://www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze for yourself or your spouse or a minor under 16: (1)full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
www.experian.com
888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA19016-0200
www.transunion.com
800-680-7289

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion,® Experian,® and Equifax,® including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)