**Washington, DC**

700 13th Street, NW, 10th Floor
Washington, DC 20005

**Brock Dahl**
**T** +1 (202) 777-4500
**T** +1 (202) 777-4538 (direct)
**E** brock.dahl@freshfields.com

**freshfields.us**

**By Email**

Office of the Attorney General

IDTheft@oag.state.md.us

March 8, 2023

To Attorney General Brown:

We write pursuant to Md. Code Ann., Com. Law § 14-3504 to inform you that Knauf Insulation, Inc. (***Knauf***) will be sending notices to Maryland residents advising them of a data incident. On or about June 29, 2022, Knauf identified indications of unauthorized access to and encryption of certain of its information technology systems. This unauthorized access resulted from a ransomware attack by a malicious actor. After discovering the incident, Knauf promptly took steps to investigate the incident in order to determine the scope of the breach, identify individuals that were impacted, and restore the integrity of the company's information systems.

A subsequent prioritized review of the contents of those systems that may have been accessed identified records of personal data potentially giving rise to a notification obligation under Maryland law. After conducting an investigation to determine the scope of the breach, Knauf has identified 47 such records for which the corresponding person appears to be a Maryland resident. By providing this notice, Knauf 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.

Although the personal information identified in connection with this incident varies from individual to individual, in general such information may include an individual's name; passport number; driver's license or other government identification number; social security number; financial account number; username and password for an online account; or health insurance information. The information may also include copies of employment files maintained by Knauf in the ordinary course of business.[1]

We are not currently aware of any financial harm to any Maryland residents whose data was involved in this incident. Knauf has alerted the Federal Bureau of Investigation of this incident and has cooperated with its investigation of the malicious actor believed to be responsible. Knauf continues to monitor and assess additional steps to maintain the security that protects its systems.

[1] Because the form individual notice submitted with this letter will be distributed in multiple states, the list of potentially impacted categories of personal information in the individual notice may include categories of information other than those on the basis of which Knauf is providing individual notice in Maryland.

Starting on March 8, formal notices of the incident will be sent by U.S. mail to individuals for whom we have identified a Maryland mailing address. A copy of the anticipated notice is attached. Knauf is providing two years of complimentary credit monitoring services to affected state residents.

Please contact me if you have any questions.

Sincerely,

/s/

Brock Dahl

Enclosures (1)

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

**Notice of Data Breach**

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to let you know about an incident in which a third party may have gained unauthorized access to your personal information. Below is a summary of what happened, what personal data was involved, what we are doing, what you can do, and where you can obtain more information.

| **Notice of Data Breach** | |
|---|---|
| What happened? | On or around June 29, 2022, certain of your personal data may have been accessed by a third party who gained unauthorized remote access to a limited number of our company systems as part of a ransomware attack.<br><br>Following discovery, we implemented measures to contain the incident and secure our network. We also began an investigation and arranged resources to start identifying, informing, and assisting persons whose personal information may have been involved. |
| What personal data was involved? | In addition to your name and information about your relationship with Knauf, the personal data that may have been accessed includes some or all the following: your date of birth; nationality; contact information; passport number; driver's license or other government identification number; social security number; financial account number; credit or debit card number; a username and password for an online account; or health insurance information. |
| What are we doing? | We are taking this incident very seriously and continue to monitor and assess additional steps to maintain the security that protects our systems. We have reported the incident to appropriate law enforcement authorities.<br><br>We have not identified any further unauthorized activity in company systems since the breach was identified in June 2022. |
| What can you do? | As a precautionary measure, we have arranged for you to enroll, at no cost to you, in an online identity monitoring service for 24 months. This service is provided by Kroll. You can find information about the service and how to activate your services in Appendix A to this letter.<br><br>In addition to enrolling in Kroll's complimentary online identity monitoring service, you can help protect yourself by monitoring your financial accounts and your account statements for unusual or unauthorized activity over the next 12 to 24 months and promptly report any suspected identity theft to the police. |
| For more information | We are sorry that this occurred. You can find more information about steps that you can take in Appendix B to this letter.<br><br>If you have questions, please call (866) 674-8834, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready. |

Yours sincerely,

Gina Max
Senior Vice President and Chief Human Resources Officer

## APPENDIX A

KROLL

### TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until* ***<<b2b_text_6(activation deadline)>>*** *to activate your identity monitoring services.*

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com

**Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

**Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## APPENDIX B

### MEASURES THAT YOU CAN TAKE TO PROTECT YOURSELF WITH REGARD TO CONSUMER CREDIT REPORTING BUREAUS:

To help protect yourself against identity theft, you may consider placing a fraud alert or security freeze on your credit report.

**Fraud Alert.** When you place a “fraud alert” on your credit report, businesses who pull your credit report will see that you may be a victim of identity theft. The company may then choose to verify your identity before they extend credit to anyone who purports to be you. This may make it harder for an identity thief to open more accounts in your name.

To place an alert, contact any one of the three main credit reporting bureaus. That company is required to tell the other two bureaus about the alert. When you first place a fraud alert on your account, it will remain for at least 90 days, after which you can renew it. When you do place an alert on your report, be sure that all three major credit reporting companies have your current contact information so they can get in touch with you.

**Security Freeze.** A “security freeze” or “credit freeze” goes further than an alert and lets you restrict access to your credit report entirely, which in turn makes it more difficult for identity thieves to open new accounts in your name. This is because most creditors need to see your credit report before they approve a new account. If creditors cannot see your file, they may not extend the credit.

A credit freeze does not affect your credit score. A credit freeze also does not:

1. prevent you from getting your free annual credit report.
2. keep you from opening a new account, applying for a job, renting an apartment, or buying insurance. But if you are doing any of these, you will need to lift the freeze temporarily, either for a specific time or for a specific party, say, a potential landlord or employer. The cost and lead times to lift a freeze vary, so it is best to check with the credit reporting company in advance.
3. prevent a thief from making charges to your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

To place a freeze on your credit reports, you need to contact each of the major credit reporting bureaus. You will need to supply your name, address, date of birth, Social Security number and other personal information. Credit reporting agencies are required to place or remove a freeze on your credit report without charge.

Below, we provide contact information for the major credit reporting agencies. You may obtain additional information from these resources about preventing or remedying identity theft, including by setting up fraud alerts or security freezes and by reviewing your credit report. The contact information of those agencies is provided below:

### EQUIFAX

**Fraud Alerts**

Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348-5069
888-836-6351 (automated service line)
800-525-6285 (customer care agents)
https://my.equifax.com/consumer-registration/UCSC/#/personal-info

**Security Freezes**

Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348-5788
888-298-0045 (customer care agents)
https://my.equifax.com/consumer-registration/UCSC/#/personal-info

**Credit Reports**

Equifax Information Services LLC
P.O. Box 740241
Atlanta, GA 30374-0241
866-349-5191
https://www.annualcreditreport.com/index.action

**EXPERIAN**

**Fraud Alerts**

Experian
P.O. Box 4500
Allen, TX 75013
1-888-397-3742
https://www.experian.com/fraud/center.html

**Security Freezes**

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013 (regular mail)

Experian
711 Experian Parkway
Allen, TX 75013 (overnight mail)

1-888-397-3742
https://www.experian.com/freeze/center.html

**Credit Reports**

Experian
P.O. Box 4500
Allen, TX 75013
1-888-397-3742
https://www.annualcreditreport.com/index.action

**TRANSUNION**

**Fraud Alerts**

TransUnion Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
888-909-8872
https://fraud.transunion.com

**Security Freezes**

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
888-909-8872
https://freeze.transunion.com/

**Credit Reports**

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281
800-888-4213
https://www.annualcreditreport.com/index.action

**INFORMATION AND ASSISTANCE THAT YOU CAN OBTAIN FROM FEDERAL AND STATE LAW ENFORCEMENT AND CONSUMER PROTECTION AGENCIES:**

If you believe that you may be the victim of identity theft, you should report that immediately to law enforcement, your state Attorney General, or the Federal Trade Commission.

You also may wish to review the resources provided by the Federal Trade Commission on how to avoid identity theft. You can reach the FTC by mail at:

Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
1-877-ID-THEFT (877-438-4338)
https://www.identitytheft.gov/

## PROTECTIONS OF THE FEDERAL FAIR CREDIT REPORTING ACT

The Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary or your major rights under the FCRA. In particular, the FCRA enables identity-theft victims to demand the removal of false entries on their credit reports that result from the theft. *For more information, including information about additional rights, go to www.ftc.gov/credit or write to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.*

**You must be told if information in your file has been used against you.** Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment or to take another adverse action against you must tell you, and must give you the name, address, and phone number of the agency that provided the information.

**You have the right to know what is in your file.** You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free disclosure if:

- a person has taken adverse action against you because of information in your credit report;
- you are the victim of identity theft and place a fraud alert in your file;
- your file contains inaccurate information as a result of fraud;
- you are on public assistance;
- you are unemployed but expect to apply for employment within 60 days.

In addition, as of September 2005 all consumers will be entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. *See www.ftc.gov/credit for additional information.*

**You have the right to ask for a credit score.** Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.

**You have the right to dispute incomplete or inaccurate information.** If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous. *See www.ftc.gov/credit for an explanation of dispute procedures.*

**Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.** Inaccurate, incomplete, or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.

**Consumer reporting agencies may not report outdated negative information.** In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.

**Access to your file is limited.** A consumer reporting agency may provide information about you only to people with a valid need—usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.

**You must give your consent for reports to be provided to employers.** A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. *For more information, go to www.ftc.gov/credit.*

**You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.** Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the lists these offers are based on. *You may opt-out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688).*

**You may seek damages from violators.** If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.

**Identity theft victims and active duty military personnel have additional rights.** *For more information, visit www.ftc.gov/credit.*

Source: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

## IF YOU ARE A RESIDENT OF CERTAIN STATES, YOU HAVE ADDITIONAL RIGHTS:

**Massachusetts**

Under Massachusetts state law, 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.

**Oregon**

You can reach the Attorney General of the State of Oregon at 1-877-877-9392 or by mail at help@oregonconsumer.gov.

**Rhode Island**

You can reach the Attorney General of the State of Rhode Island by phone at (401) 274-4400 or online at www.riag.ri.gov.

**Maryland**

You may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or calling 1-410-576-6491. The Identity Theft Unit can give you step-by-step advice on how to protect yourself from identity thieves using, or continuing to use, your personal information. You may also reach the Maryland Attorney General by mail at:

Identity Theft Unit
Office of the Attorney General
200 St. Paul Place
25th Floor
Baltimore, MD 21202

**North Carolina**

You can reach the Attorney General of the State of North Carolina by mail at:

9001 Mail Service Center
Raleigh, NC 27699-9001
+1 (919) 716-6400
http://www.ncdoj.gov

**District of Columbia**

You can reach the Attorney General of the District of Columbia at:

400 6th Street NW
Washington, D.C. 20001
Phone: (202) 727-3400
https://oag.dc.gov/