

Dominic A. Paluzzi
Direct Dial: 248.220.1356
Email: dpaluzzi@mcdonaldhopkins.com

August 30, 2024

VIA EMAIL: Idtheft@oag.state.md.us

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Daubert Chemical Company, Inc. – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Daubert Chemical Company, Inc. (“Daubert”) regarding a recent security incident. I am writing to provide notification of an incident at Daubert that may affect the security of personal information of approximately three (3) Maryland residents. Daubert will supplement this notification with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Daubert does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about May 3, 2024, Daubert detected unauthorized access to its network. Upon learning of this issue, Daubert immediately took steps to secure the network and mitigate against any additional harm. As part of its investigation, Daubert engaged external cybersecurity professionals experienced in handling these type of incidents to conduct an investigation. After an extensive forensic investigation and thorough manual review, Daubert determined on August 13, 2024 that certain impacted files containing personal information of individuals may have been acquired in connection with this incident. The personal information impacted includes full name, Social Security number, driver’s license and/or government issued identification number, digital signature, passport number, date of birth, and salary information. The impacted elements of information varied per individual.

To date, Daubert is not aware of any reports of identity fraud or financial fraud for any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Daubert wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Daubert is providing the affected residents with notification of this incident, commencing on or about August 30, 2024. The notice will be in substantially the same form as the letter attached hereto. Daubert is also offering the affected residents with complimentary credit-monitoring services, as their Social Security Numbers were potentially impacted. Daubert is advising the affected residents to always remain vigilant in reviewing financial account statements and credit reports for fraudulent or

irregular activity on a regular basis. Daubert is also advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Finally, the affected residents are being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Daubert, protecting the privacy of personal information is a top priority. Daubert is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Further, Daubert continues to evaluate and improve, where appropriate, its administrative and technical safeguards including training its employees on best practices related to cybersecurity, policies, procedures, and protocols, and tools to protect its network environment.

Should you have any additional questions, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Thank you for your cooperation.

Sincerely,



Dominic A. Paluzzi



IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Daubert Chemical Company, Inc. ("Daubert"). We are writing with important information regarding a recent data security incident that potentially involved some of your information. We want to provide you with information about the incident, inform you about the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about May 3, 2024, Daubert experienced unauthorized access to our network.

What We Are Doing.

Upon learning of this issue, Daubert immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we determined on August 13, 2024, that certain impacted files containing personal information may have been accessed and acquired by an unauthorized individual(s).

What Information Was Involved.

The potentially impacted information may include your [REDACTED]

[REDACTED] Please note, not all data elements were necessarily impacted for every individual receiving this notice as part of this incident.

What You Can Do.

To date, we are not aware of any reports of identity fraud or improper use of your information as a result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To help protect your identity from any potential misuse of your information, we have secured the services of Kroll to provide identity monitoring at no cost to you for 24 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have been impacted by an unintentional exposure of personal data. Your identity monitoring service includes Credit Monitoring, Fraud Consultation and Identity Theft Restoration. To activate this free service, please see the "Other Important Information" section.

This letter also provides other standard precautionary measures you can take to help protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. Daubert remains fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have questions regarding this letter or identity monitoring activation, please call [REDACTED]
[REDACTED] Please have your membership
number ready. For any additional questions regarding this incident, please contact [REDACTED]
at [REDACTED] [REDACTED]
[REDACTED]

Sincerely,

Daubert Chemical Company, Inc.

4700 S. Central Ave.

Chicago, IL 60638

– OTHER IMPORTANT INFORMATION –

1. **Activating the Complimentary 24-Month Identity Monitoring.**

How to Activate Your Identity Monitoring Service:

Visit [REDACTED] to activate and take advantage of your identity monitoring services.

You have until [REDACTED] to activate your identity monitoring services.

Membership Number: [REDACTED]

For more information about Kroll and your Identity Monitoring services, you can visit [REDACTED]

Additional information describing your services is included with this letter.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring.

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—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 can help you determine if it's 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 can 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.

2. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one (1) credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013

<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000

Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. **Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(888)-298-0045

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

(888) 397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

<https://www.transunion.com/credit-freeze>

(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one (1) free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report 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.

New Jersey Residents: You may obtain information about preventing identity theft from the New State Police: P.O. Box 7068, West Trenton, NJ 08628; <https://nj.gov/njsp/tech/identity.html>; Telephone: 609-882-2000.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392.