CLEARY GOTTLIEB STEEN & HAMILTON LLP

One Liberty Plaza
New York, NY 10006-1470
T: +1 212 225 2000
F: +1 212 225 3999

clearygottlieb.com

D: +1 212-225-2912
rmukhi@cgsh.com

May 31, 2024

VIA E-MAIL
Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown:

Pursuant to Maryland Personal Information Protection Act § 14-3504, we write on behalf of our client, Mermet USA (together, the "Company" or "Mermet"), to notify you of a cybersecurity incident involving approximately one (1) Maryland resident.

IDENTIFICATION OF PARTIES

The entity that experienced the incident is Mermet USA, which is a U.S.-based manufacturer of vinyl coated fiberglass sunscreen fabrics. Mermet's headquarters are located at 5970 North Main Street, Cowpens, South Carolina 29330.

NATURE OF THE DATA SECURITY INCIDENT

On March 12, 2024, Mermet USA experienced an IT disruption. Following the Company's incident response process, Mermet immediately launched an internal investigation and engaged third-party experts to protect the Company's data, minimize incident impact, and bring the Company's systems back online as quickly as possible. These experts have determined it was a ransomware attack. The Company quickly contained the incident and eradicated any elements of the attack, and, with the guidance of external experts, we believe we have also identified and remediated the root causes of the incident.

Through the forensic investigation, the Company learned that certain data was accessed and obtained by the threat actor.

NUMBER OF INDIVIDUALS

Maryland Residents: One (1)

In May 2024, Mermet USA's investigation determined that one Maryland resident's personal information was impacted. The personal information included the individual's Social Security number, date of birth, and medical and health insurance information may also have been impacted. Mermet USA expects to notify that Maryland resident as early as possible in June 2024. Notice has not been delayed due to a law enforcement investigation. A sample copy of the notice is attached hereto.

STEPS MERMET HAS TAKEN OR PLANS TO TAKE RELATING TO THE INCIDENT

Mermet has taken a number of steps to address the incident, and its work remains ongoing. As noted above, upon discovery of the incident, the Company's cybersecurity team immediately took a series of steps—e.g., steps intended to contain the incident, hiring cybersecurity experts, conducting an investigation to identify and remove any malicious files, and determine Company systems that were impacted—as well as steps seeking to implement measures to fortify our defenses going forward.

CREDIT MONITORING

Mermet is offering 24 months of identity theft and credit monitoring services to the affected Maryland resident free of charge. A sample of the letter to be sent to the affected resident offering these services is attached hereto. A description of the services is available here: https://www.experianidworks.com.

CONTACT INFORMATION

You may contact me at 212-225-2912 or rmukhi@cgsh.com should you have any questions or need further information.

Respectfully submitted,

Rahul Mukhi

Rahul Mukhi

Attachment

Sun Control Textiles™

DRAFT

June [[X]], 2024

[[Insert Recipient's Name]]
[[Insert Address]]
[[Insert City, State, Zip]]

RE: Notice of Cybersecurity Incident
Please read this entire letter.

To [[Impacted Individual's Name]]:

I write on behalf of Mermet USA (the "Company" or "we") to inform you of a cybersecurity incident involving some of your personal information. We take the protection of your information very seriously, and we are contacting you directly to explain the circumstances of the incident and the steps we are taking in response.

What Happened?

On March 12, 2024, the Company experienced an IT disruption. Following our incident response process, we immediately launched an internal investigation and engaged third-party experts to protect our data, minimize incident impact, and bring our systems back online as quickly as possible. These experts have determined it was a cybersecurity incident.

Through the third-party investigation, we learned that certain data may have been accessed and obtained without authorization by the third-party threat actor. We quickly contained the incident and eradicated any elements of the attack, and, with the guidance of external experts, we believe we have also identified and remediated the root causes of the incident.

What Information Was Involved?

The Company maintains personal information on its systems that was determined to be accessed and obtained by an unauthorized third party as part of the incident.

The Company's investigation recently determined that some of your personal information was impacted, including your [[insert the Recipient's specific information that we know was impacted]]. In addition, medical and health insurance information about you may have been impacted. The information about you that was impacted by the incident depends on, among other things, the particular information that was provided to the Company.

What We Are Doing To Protect Your Information

Please be assured that we are doing everything we can to address the incident. Upon discovery of the incident, our cybersecurity team immediately took a series of steps, including steps intended to contain the incident, hiring cybersecurity experts, conducting an investigation to identify and remove any malicious files and determine Company systems that were impacted, as well as steps seeking to implement measures to fortify our defenses going forward.

Protecting your personal information is very important to us. To help protect your personal information, we are providing you, at no cost, with identity theft detection and resolution tools through Experian, one of the leading credit and identity monitoring companies, through a complimentary 24-month membership to Experian's® IdentityWorks℠.

To activate this membership and start monitoring your personal information, please follow the steps in Attachment 1.

What You Can Do

We want to make sure you are aware of the additional steps you may take to guard against the unauthorized use of your personal information.

As we all know, cybersecurity incidents increasingly threaten the security of information at work and at home. You should remain vigilant by reviewing account statements and monitoring free credit reports. Please see Attachment 2 for further steps you can take to protect your personal information as well as additional important information. We also encourage you to report any suspicious computer-related activity.

Conclusion

As noted, please see the attachments for instructions on how to enroll in Experian's® IdentityWorks℠, further steps you can take to protect your personal information, and additional important information.

We regret any inconvenience that the incident may cause. Should you have questions or concerns regarding this matter, please call [[Experian Helpline Number]] Monday through Friday, 8:00 a.m. to 8:00 p.m. CST (excluding major U.S. holidays).

Sincerely,
Chris Duerk
Managing Director

ATTACHMENT 1

How To Enroll In Experian's® IdentityWorks^{SM}

- Ensure that you **enroll by**: [[enrollment end date]]. Your **activation code** will not work after this date.
- **Visit** the Experian IdentityWorks website to enroll: [[URL]]
- Provide your **activation code**: [[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 [[customer service number]] by [[enrollment end date]]. Please be prepared to provide engagement number [[engagement #]] as proof of your eligibility for IdentityWorks.

Additional Details Regarding the 24-Month Experian IdentityWorks Membership

A credit card is **not** required for enrollment in Experian IdentityWorks. You may contact Experian **immediately** regarding any fraud issues, and you 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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE^{TM}:** You will receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance[1]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your personal information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [[customer service number]]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent will be available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

[1] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Please note that Identity Restoration support is available as part of the membership being provided at no cost to you and is effective from the date of this letter. Registration is not required to access the service provided by Experian's Identity Restoration Specialists. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

ATTACHMENT 2

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®	**Experian**	**TransUnion®**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as a home address or Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a 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 access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com/personal/credit-report-services	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts one (1) year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com/personal/credit-report-services	www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statements that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

- California Residents: The California Office of Privacy Protection can be contacted at 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; or www.oag.ca.gov/privacy.

- Georgia Residents: The Attorney General can be contacted at 2 Martin Luther King Jr. Drive, Suite 356, Atlanta, GA 30334-9077; 800-869-1123; or https://consumer.georgia.gov/consumer-topics/identity-theft-what-do-if-it-happens-you.

- Illinois Residents: The Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-800-386-5438; or https://ccformsubmission.ilag.gov/.

- Maryland Residents: The Attorney General can be contacted at 200 St. Paul Place, 25th Floor, Baltimore, MD 21202: 410-576-6491; or https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx. Further information about security breach response and identity theft prevention and protection can be obtained from Maryland's Office of the Attorney General.

- New Jersey Residents: The Attorney General can be contacted at 124 Halsey Street, Newark, NJ 07101; 973-504-6200; or https://www.njconsumeraffairs.gov/ocp/Pages/default.aspx.

- North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6000; or https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-your-business-from-id-theft/security-breach-information/security-breachadvice/. Further information about preventing identity theft can be obtained from North Carolina's Office of the Attorney General.

- South Carolina Residents: The Attorney General Consumer Affairs Division can be contacted at 293 Greystone Boulevard, Suite 400; 803-734-4200; or https://consumer.sc.gov/identity-theft-unit.