

[REDACTED]

[REDACTED]

Dear Attorney General Brown,

I am writing to inform you about a security incident affecting **two (2)** Maryland residents.

Good afternoon. Our firm represents the Sporting Goods Division of Mitsubishi Chemical America, Inc. ("MCA"), which experienced a security incident, and we are hereby formally notifying you of this event pursuant to Md. Code Ann. Com. Law § 14-3504 (West 2022). By providing this notice, MCA does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland notification security breach statute, or all/any other applicable laws (including those pertaining to personal jurisdiction).

On May 19, 2023, the Sporting Goods Division of MCA learned that it was the target of a ransomware attack by an unknown third party. We quickly launched an investigation to determine the nature and scope of the activity, working with cybersecurity experts to determine what happened and what information may have been affected. The investigation identified that the threat actor gained unauthorized access to our servers. We immediately commenced a thorough review to determine whether sensitive information was present in the impacted data. On June 19, 2023, the investigation concluded that some personal information might have been included among information accessed by the threat actors. We have used the information in our recovered files to identify the most recent contact information for those affected.

Potentially exposed records included the name, address, date of birth, Social Security number, telephone number, email address, driver's license or identification document information, tax information, pay information, and financial account information of current and former employees, as well as credit card information of customers. To date, we have not received any reports of actual or attempted misuse of this information.

Upon discovering the incident, MCA took immediate steps to investigate and contain the attack and identify those who may have been affected. MCA worked with computer forensics experts to identify the information accessed, ensure that the threat actors no longer have access to our systems and data, and

safeguard against future unauthorized access to our systems and information. MCA reviewed the contents of the impacted systems to determine whether they contained personal information, identifying contact information, and using that information to provide notice to potentially affected individuals.

As additional security measures and to help prevent such an incident in the future, MCA blocked known malicious IPs used by the threat actor and forced password changes across all personnel. The company also expanded the use of multi-factor authentication (“MFA”) to all single-sign-on services wherever technically feasible and enhanced logging and monitoring capabilities. Enhanced monitoring included additional EDR/XDR functionality, 24/7 monitoring by external vendors, and scanning for relevant Dark Web activity.

Very respectfully,

Charles E. Westerhaus, CIPP/US/E, CIPM

Associate

charles.westerhaus@faegredrinker.com

Connect: vCard

+1 317 569 4852 direct

Faegre Drinker Biddle & Reath LLP

600 E. 96th Street, Suite 600

Indianapolis, Indiana 46240, USA

This message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message and any attachments.

NOTICE OF DATA BREACH

July , 2023

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

RE: NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>,

The Sporting Goods Division of Mitsubishi Chemical America, Inc. (“MCA”) writes to inform you about a recent cybersecurity incident that may affect the security of some of your information. Safety is a core value of MCA, and we take your security and the security of your personal information very seriously. Out of an abundance of caution, we are providing this notice to explain what we understand has happened and to outline steps you may take to help protect yourself.

What Happened? On May 19, 2023, the Sporting Goods Division of MCA learned that it was the target of a ransomware attack by an unknown third party. We quickly launched an investigation to determine the nature and scope of the activity, working with cybersecurity experts to determine what happened and what information may have been affected. The investigation identified that the threat actor gained unauthorized access to our servers. We immediately commenced a thorough review to determine whether sensitive information was present in the impacted data. On June 19, 2023, the investigation concluded that some of your information might have been included among information accessed by the threat actors. We have used the information in our recovered files to identify the most recent contact information for those affected.

What Information Was Involved? We are notifying you out of an abundance of caution because information related to you was identified in the files that the threat actor potentially accessed. The information related to you that was potentially accessed may include, among other things, your name, address, date of birth, Social Security number, telephone number, email address, driver’s license or identification document information, tax information, pay information, and financial account information. To date, we have not received any reports of actual or attempted misuse of your information.

What We Are Doing. We take this incident and the security of information in our care very seriously. When we learned of this incident, MCA took immediate steps to investigate and contain the attack and identify those who may have been affected. We have been working with industry-leading computer forensics experts to identify the information accessed, ensure that the threat actors no longer have access to our systems and data, and safeguard against future

unauthorized access to our systems and information. We reviewed the contents of the impacted systems to determine whether they contained personal information, identifying contact information, and using that information to provide notice to potentially affected individuals. We are committed to the security of all information in our care and are reviewing existing policies and procedures to protect against a similar future incident.

We do not have any information to suggest that your personal information has been used inappropriately or without authorization. However, to protect against identity theft, we have arranged to make available to you [24 months] of identity theft resolution services provided by Experian's® IdentityWorksSM at no charge. Please note that you must enroll to take advantage of this free service, and we encourage you to do so.

This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure you **enroll by: [insert date]** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code: [insert code]**

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, don't hesitate to contact Experian's customer care team at their customer service number at 877-890-9332. Be prepared to provide engagement number **[insert number]** as proof of eligibility for the identity restoration services by Experian.

What Can You Do?

Again, we do not believe this incident presents an immediate risk to you, and we have no evidence that your personal information has been misused. We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your credit reports and financial or health statements for unauthorized activities. Also, please review the enclosed attachment called *Preventing Identity Theft and Fraud* for more information on ways to protect against the potential misuse of your information.

Additional details regarding your 24-MONTH EXPERIAN IDENTITYWORKS Membership:

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

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 ExtendCARE™:** You receive the same high-level Identity Restoration support even after your Experian IdentityWorks membership expires.
- **Up to \$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is 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).

Please note that this Identity Restoration support is available to you for one year from the date of this letter, and you can enroll at any time during that period. 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 on this site.

For More Information

Again, we take your privacy seriously and regret any concern or inconvenience this incident may cause you. If you have additional questions, please contact Joseph Sherinsky, at joseph.sherinsky@mcgc.com or (212) 672-9432.

PREVENTING IDENTITY THEFT AND FRAUD

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Immediately report any suspicious activity to your bank or credit union and call your local police or sheriff's office, or state Attorney General and file a report of identity theft. You have a right to a copy of the police report, and you may need to give copies of the police report to creditors to clear up your records and access some services free to identity theft victims.

Under the U.S. Fair Credit Reporting Act and other laws, you have certain rights that can help protect yourself from identity theft. Many of these are explained in this document and at [www.identitytheft.gov/ Know-Your-Rights](http://www.identitytheft.gov/Know-Your-Rights). For example, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can have these credit bureaus place a short-term or an extended "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert or have any questions regarding your credit report, please contact any of the agencies listed below.

Equifax (866) 349-5191 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com P.O. Box 2002 Allen, TX 75013	TransUnion (800) 888-4213 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19016
---	--	---

You may also place a security freeze on your credit reports free of charge. A security freeze, also known as a "credit freeze," prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. But unlike a fraud alert, you must place a security freeze separately on your credit file at **each** bureau. You can use the following addresses and contact information to place a security freeze with each major credit bureau:

Equifax Security Freeze. 1-800-685-1111. P.O. Box 1057881, Atlanta, GA 30348-0241.
www.equifax.com/personal/credit-report-services/credit-freeze/;

Experian Security Freeze. 1-888-EXPERIAN or 1-888-397-3742. P.O. Box 9554, Allen, TX 75013. www.experian.com/freeze/center.html; or

TransUnion. 1-800-680-7289. Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000. www.transunion.com/credit-freeze

In order to request a security freeze, you may need to supply your full name (including middle initial, as well as Jr., Sr., II, III, etc.), date of birth, Social Security number, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement to show proof of your current address. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning your identity theft. The credit reporting agencies must place a security freeze on your credit report within one (1) business day after receiving a request by phone or secure electronic means and within (3) business days after receiving your request by mail. The credit bureaus must then send written confirmation to you within five (5) business days of placing the security freeze, along with information about how to remove or lift the security freeze in the future.

You can further educate yourself regarding identity theft, fraud alerts, freezes, and the steps you can take to protect yourself by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission encourages those who discover their information has been misused to file a complaint with them.

The Federal Trade Commission can be reached at:

Federal Trade Commission
Consumer Resource Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.identitytheft.gov or www.ftc.gov

OTHER IMPORTANT INFORMATION

You may also file a report with your local police or the police in the community where the identity theft took place. Further, you are entitled to request a copy of the police report filed in this matter.

For California residents:

You can visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Maryland residents:

You may obtain information about avoiding identity theft at: Office of the State of Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023
www.marylandattorneygeneral.gov

For Washington D.C. residents:

You may obtain information about avoiding identity theft at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 202-727-3400,
<https://oag.dc.gov/>

For Maryland and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For Rhode Island residents:

Rhode Island residents may request additional information by contacting the Rhode Island, Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401)274-4400.]

For North Carolina residents:

North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/> or at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000