



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Brittany R. Bickel
Office: (267) 930-1129
Fax: (267) 930-4771
Email: BBickel@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

June 27, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent The Ultra-Met Company (“Ultra-Met”) located at 720 North Main Street, Urbana, Ohio 43078, and are writing to notify your office of an incident that may affect the security of certain personal information relating to three (3) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Ultra-Met 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.

Nature of the Data Event

On March 13, 2023, Ultra-Met became aware of suspicious activity affecting certain systems within its network. Ultra-Met moved quickly to secure the network and began an investigation with the assistance of third-party forensic specialists to identify what happened and confirm what information may have been involved. The investigation determined that an unknown actor gained access to certain Ultra-Met systems on or about March 13, 2023, and took certain information stored in those areas.

Ultra-Met then undertook a review of the files stored on its systems to determine what information was contained therein and to whom it related. This review was completed on or around May 17, 2023. Thereafter, Ultra-Met then conducted additional review of its internal records to confirm the identities and contact information for affected individuals. This was recently completed and identified that certain information relating to Maryland residents was present in files stored on Ultra-Met’s systems that were accessed by an unknown actor.

Mullen.law

The information that was subject to unauthorized access relating to Maryland residents includes name and Social Security number.

Notice to Maryland Residents

On or about June 27, 2023, Ultra-Met provided written notice of this incident to three (3) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Ultra-Met moved quickly to investigate and respond to the incident, assess the security of Ultra-Met systems, and identify potentially affected individuals. Further, Ultra-Met notified federal law enforcement regarding the event. Ultra-Met is also working to implement additional safeguards and training to its employees. Ultra-Met is providing access to credit monitoring services for two (2) years, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Ultra-Met is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Ultra-Met is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1129.

Very truly yours,

A handwritten signature in cursive script, reading "Brittany Bickel".

Brittany R. Bickel of
MULLEN COUGHLIN LLC

EXHIBIT A

Ultra-met[®]

carbide technologies

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

June 27, 2023

J6156-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L02 FORMER EMP & DEP



APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



NOTICE OF [Extra1]

Dear Sample A. Sample:

The Ultra-Met Company (“Ultra-Met”) writes to notify you of a recent event that may have impacted some of your information. We are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On March 13, 2023, Ultra-Met became aware of suspicious activity affecting certain systems within our network. We moved quickly to secure the network and began an investigation with the assistance of third-party forensic specialists to identify what happened and confirm what information may have been involved. The investigation determined that an unknown actor gained access to certain Ultra-Met systems on or about March 13, 2023, and took certain information stored in those areas.

Following the investigation, we then undertook a thorough and time-intensive review of the involved files for sensitive information. This review was recently completed. Thereafter, we conducted additional review of our files to identify contact information for the impacted individuals to provide this notification.

What Information Was Involved? Our investigation determined that the following types of your information were included in the involved files: your [Extra2].

What We Are Doing. Safeguarding the privacy of information in our care and the security of our network are among our highest priorities. Upon learning of this event, we moved quickly to investigate and respond, assess the security of our systems, and notify potentially affected individuals. We promptly notified the Federal Bureau of Investigation of this event. As part of our ongoing commitment to the security of information within our care, we are reviewing our existing policies and procedures regarding cybersecurity and evaluating additional measures and safeguards to protect against this type of event in the future. We also implemented additional network security measures to further enhance our network security.

Although we are unaware of any misuse of your information as a result of this incident, as an added precaution, we are offering you complimentary access to two (2) years of credit monitoring services through Experian. For details of this offer and enrollment instructions, please review the information contained in the attached *Steps You Can Take to Protect Personal Information*.

B096274

0000002



J6156-L02

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Protect Personal Information*. There, you will find more information on the credit monitoring and identity restoration services we are making available to you. We encourage you to activate these services as we are not able to act on your behalf to do so.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our toll-free dedicated assistance line at (888) 397-0035 , Monday through Friday 9:00 a.m. – 11:00 p.m. Eastern Time, excluding U.S. holidays. You may also write to Ultra-Met at 720 North Main Street, Urbana, OH 43078.

Sincerely,

The Ultra-Met Company

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services and Resolution Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months at no cost to you.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: September 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (888) 397-0035 by September 30, 2023. Be prepared to provide engagement number B096274 as proof of eligibility for the Identity Restoration services by Experian.

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 ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** 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.



Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity

theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 0 Rhode Island residents impacted by this incident.

