



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Brian F. Fox
Office: (267) 930-4777
Fax: (267) 930-4771
Email: bfox@mullen.law

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

November 7, 2022

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

Dear Sir or Madam:

We represent Metropolitan Associates located at 1123 N. Astor Street, Milwaukee, WI 53202, and are writing to notify your office of an incident that may affect the security of certain personal information relating to thirteen (13) Maryland residents. This notice may be supplemented if significant new facts are learned subsequent to its submission. By providing this notice, Metropolitan Associates 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 29, 2022, Metropolitan Associates identified suspicious activity relating to certain computer systems and immediately launched an investigation with the help of industry-leading cybersecurity specialists to determine the nature and scope of the activity. Metropolitan Associates quickly worked to secure their systems, restore access to the information so Metropolitan Associates could continue to operate without disruption, and investigate what happened and whether the event resulted in any unauthorized access to, or theft of, information by the unknown actor.

Through the investigation, Metropolitan Associates determined that an unauthorized actor may have gained access to certain computer systems within the Metropolitan Associates network between March 26, 2022 to March 29, 2022. The unauthorized actor may have viewed or downloaded certain files from those systems.

Metropolitan Associates then worked with third-party data review specialists to perform a comprehensive programmatic and manual review of the data stored on the affected systems to determine what information was impacted and to whom the information related. Upon completion of the review, Metropolitan Associates conducted a time-intensive manual review of its records to determine the identities and contact information for potentially affected individuals.

Mullen.law

The information that could have been subject to unauthorized access for Maryland residents includes name, Social Security number, and financial account information. The information potentially subject to unauthorized access varies for each affected individual.

Notice to Maryland Residents

On or about November 7, 2022, Metropolitan Associates provided written notice of this incident to thirteen (13) 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, Metropolitan Associates moved quickly to investigate and respond to the incident, assess the security of Metropolitan Associates systems, and identify potentially affected individuals. Metropolitan Associates is also assessing whether additional safeguards might be available for implementation to enhance the security of its computer systems to reduce the likelihood of a similar future event. Metropolitan Associates is providing access to credit monitoring services for one (1) year, through Transunion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Metropolitan Associates 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. Metropolitan Associates is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. Metropolitan Associates also notified other appropriate state regulators and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4777.

Very truly yours,

Brian F. Fox of
MULLEN COUGHLIN LLC

BFF/kml
Enclosure

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA <<Variable Header>>

Dear <<Name 1>>:

Metropolitan Associates is writing to notify you of a data security event that may have impacted the security of some of your information. We are providing you with information about the event, our response to it, and information related to what you may do to better protect your information, should you feel it is appropriate to do so.

What Happened? On March 29, 2022, Metropolitan Associates identified suspicious activity relating to certain computer systems and immediately launched an investigation with the help of industry-leading cybersecurity specialists to determine the nature and scope of the activity. The investigation determined that an unauthorized actor may have gained access to certain computer systems within the Metropolitan Associates network between March 26, 2022 to March 29, 2022. The unauthorized actor may have viewed or taken information stored on those systems.

The investigation was unable to confirm which specific files may have been viewed or taken by the unauthorized actor. As a result, we are unable to rule out that some of your information stored in our systems may have been at risk. We therefore undertook a thorough and time-intensive review of all potentially involved files to determine if they contained sensitive information. The review was recently completed and information related to you was identified within the data set.

What Information Was Involved? The following types of your information may have been impacted: <<Breached elements>> and your name.

What We Are Doing. Metropolitan Associates has strict security measures in place to protect information in our care. In addition to investigating this incident with assistance from industry-leading cybersecurity specialists, Metropolitan Associates worked quickly to identify opportunities to enhance existing security processes to reduce the likelihood of similar future events.

As an additional precaution, Metropolitan Associates is offering you access to <<CM Length>> months of complimentary credit monitoring services through Transunion. Details of this offer and instructions on how to activate these services are enclosed with this letter.

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. Please review the enclosed "Steps You Can Take to Help Protect Your Information," which contains information on what you can do to better safeguard against possible misuse of your information.

For More Information. We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 855-934-1694. This toll-free line is available Monday – Friday from 8:00 am to 8:00 pm Central Time.

We sincerely regret the inconvenience this event may cause you. We remain committed to safeguarding the information in our care and will continue to take steps to ensure the security of our systems.

Sincerely,

Metropolitan Associates Management

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring & Identity Restoration

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for <<CM Length>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at **www.mytrueidentity.com** and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code <<**Activation Code**>> and follow the three steps to receive your creditmonitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code << **Insertstatic 6-digit Telephone Pass Code** >> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain <<CM Length>> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *myTrueIdentity* online Credit Monitoring service anytime between now and <<**Enrollment Deadline**>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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
888-298-0045	1-888-397-3742	833-395-6938
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. You may obtain information from these sources and/or the Federal Trade Commission using the contact information noted above about steps you can take to avoid identity theft. You can write to Metropolitan Associates at the following address: 1123 N. Astor Street, Milwaukee, WI 53202-3326.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You 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 you to review your 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 Avenue NW, 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 <<#>> Rhode Island residents impacted by this incident.