

December 1, 2023

Via E-Mail: Idtheft@oaq.state.md.us

Attorney General Anthony Brown
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Cybersecurity Incident

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Montachusett Regional Vocational Technical School District (“Monty Tech”), an independent regional vocational-technical school, in Fitchburg, MA, with respect to a cybersecurity incident that was discovered by Monty Tech on October 8, 2023 (hereinafter, the “Incident”). Please note Monty Tech takes the security and privacy of the information within its control seriously, and has taken steps to reduce the likelihood of a similar incident from occurring in the future. This letter will serve as a notice of the Incident and to inform you of the steps Monty Tech has taken in response to the Incident.

1. Nature of the Incident

On October 6, 2023, Monty Tech was made aware that its computer systems had been impacted by a ransomware incident resulting in the encryption of its computer systems (the “Incident”). Immediately upon discovery of the Incident, Monty Tech engaged a specialized incident response vendor to conduct a forensic investigation to determine the extent and root cause of the incident. The forensic investigation concluded on November 8, 2023, which confirmed unauthorized access to Monty Tech’s computer systems.

Upon confirming unauthorized access to its systems, Monty Tech conducted a review of the compromised servers to determine whether personally identifiable information was maintained within the impacted computer servers for purposes of notifying those individuals whose sensitive personal information may have been impacted by the Incident. Based on its review of the data maintained within the compromised computer systems, Monty Tech determined that the following elements of personal information may have been accessed and/or acquired by an unauthorized individual: names, dates of birth, license information, and Social Security numbers.

400 Poydras Street, Suite 2250 | New Orleans, LA 70130 | p 504.702.1710 | f 504.702.1715 | wilsonelser.com

Albany, NY | Atlanta, GA | Austin, TX | Baltimore, MD | Beaumont, TX | Birmingham, AL | Boston, MA | Charlotte, NC | Chicago, IL | Dallas, TX | Denver, CO
Detroit, MI | Edwardsville, IL | Garden City, NY | Hartford, CT | Houston, TX | Jackson, MS | Las Vegas, NV | London, England | Los Angeles, CA | Louisville, KY
Madison, NJ | McLean, VA | Merrillville, IN | Miami, FL | Milwaukee, WI | Nashville, TN | New Orleans, LA | New York, NY | Orlando, FL | Philadelphia, PA | Phoenix, AZ
Raleigh, NC | San Diego, CA | San Francisco, CA | Sarasota, FL | Seattle, WA | Stamford, CT | St. Louis, MO | Washington, DC | West Palm Beach, FL | White Plains, NY

To mitigate the incident, Monty Tech mailed notification letters to the potentially affected individuals along with an offer for complimentary credit monitoring services and further instructions on how to protect their personal information. As of this writing, Monty Tech has not received any reports of related identity theft, since the date of the Incident to the present.

2. Number of Maryland residents affected.

Monty Tech discovered that the Incident may have resulted in unauthorized exposure of information pertaining to one (1) Maryland resident. Notification letter to this individual was mailed on December 1st, 2023, by First Class Mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Monty Tech is committed to ensuring the security and privacy of all personal information within its control. Upon discovery of the Incident, Monty Tech moved quickly to investigate and respond to the Incident. Specifically, Monty Tech engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, Monty Tech has taken steps to strengthen its security posture to reduce the likelihood of a similar incident from occurring in the future.

Monty Tech is also offering twelve (12) months of complimentary credit monitoring and identity theft restoration services through TransUnion to potentially affected individuals residing in Maryland to help protect their identity. Additionally, Monty Tech provided guidance on how to better protect against identity theft and fraud, including providing 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 the contact details for the Federal Trade Commission.

4. Contact Information

Monty Tech remains dedicated to protecting the sensitive information within its control. Should you have any questions or need additional information, please do not hesitate to contact me at dominik.cvitanovic@wilsonelser.com or 504.372.6698

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

A handwritten signature in blue ink, appearing to read "D. Cvitanovic", is positioned above the printed name.

Dominik J. Cvitanovic, Esq.

EXHIBIT A



December 1, 2023

Dear _____ :

Montachusett Regional Vocational Technical School District (“Monty Tech”) is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your sensitive personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with steps we are taking in response, and resources available to help you protect against the potential misuse of your information. Please be assured that Monty Tech takes the protection and proper use of your personal information very seriously.

What Information Was Involved?

The following data was acquired by a person not authorized to view them: name, date of birth, and SSN.

What We Are Doing?

Data security is one of our highest priorities. Upon detecting this incident, we moved quickly to initiate an investigation, which included retaining a leading forensic investigation firm who assisted in conducting an investigation and confirming the security of our network environment.

We also deployed additional monitoring tools and will continue to enhance the security of our systems. We take the protection and proper use of personal information very seriously.

As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident, and we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

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 or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit

Montachusett Regional Vocational Technical School does not discriminate on the basis of race, color, sex, gender identity, religion, national origin, sexual orientation, disability, homelessness, or limited English proficiency.

bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

To enroll in Credit Monitoring services at no charge, please log on to **<https://secure.identityforce.com/benefit/mrvtsd>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **TJQEUAA** Please note that the code is case-sensitive and will need to be entered as it appears.

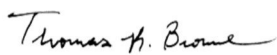
In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Once enrolled you will have twenty-four (24) months of monitoring services. At the end of twenty-four (24) months, the services will be deactivated. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line 1-844-958-5317 and supply the fraud specialist with the unique code listed above. The call center representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your child or dependent's personal information.

At Monty Tech, we take our responsibilities to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,



Thomas R. Browne
Superintendent-Director

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600