Jennifer S. Stegmaier
312.821.6167 (direct)
jennifer.stegmaier@wilsonelser.com

July 24, 2024

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

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

Re: Data Security Incident Involving Marathon County Special Education

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Marathon County Special Education ("MCSE"), a special education programs and services provider located at 1200 Lake View Dr, #35, Wausau, WI 54403, with respect to a recent data incident that was first discovered by MCSE on October 20, 2023 (hereinafter, the "Incident"). MCSE takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, and the steps that MCSE has taken in response to the Incident. We have also enclosed hereto a sample notice letter mailed to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On October 20, 2023, MCSE detected unauthorized activity within its e-mail environment. Upon discovery of the Incident, MCSE promptly engaged a specialized cybersecurity firm to secure its environment and investigate the nature and scope of the unauthorized activity. On December 19, 2023, the forensic investigation concluded that current and former MCSE student personally identifiable information may have been accessed by an unauthorized user. Based upon the results of the forensic investigation, MCSE engaged a third-party data mining company to conduct a review of the impacted data in order to determine which student information may have been impacted. MCSE completed its review of the impacted data on April 9, 2024.

Based upon the results of the investigation MCSE determined that an unauthorized user may have had access to the following types of information: names, addresses, dates of birth, medical treatment/procedure information, and provider names.

At this time, MCSE has not received any reports of identity theft or misuse of personal information resulting from this Incident.

2. Number of Maryland residents affected.

Based upon the investigation, on May 30, 2024, MCSE mailed a first wave of notification letters to the individuals whose data was maintained with the compromised systems along with an offer for complimentary credit monitoring services. A second wave of notifications to the individuals was mailed on July 8, 2024. No impacted Maryland residents were included in the first and second rounds of notification.

Upon further review of the impacted information, MCSE identified and notified two (2) Maryland residents whose information was impacted as a result of the incident. A third wave of notice letters was mailed on July 19, 2024, by U.S. First Class Mail. A sample copy of the notification letter sent to the affected Maryland residents in the third wave of notification is attached hereto as **Exhibit A**.

3. Steps taken in response to the Incident.

MCSE is committed to ensuring the security and privacy of all personal information in its control and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, MCSE moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, MCSE engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, MCSE administered additional training for its employees and implemented additional technical and administrative safeguards with respect to safeguarding sensitive data within its control. MCSE also informed our law firm for the purpose of identifying the potentially affected individuals in preparation for notice.

To further mitigate any potential harm, MCSE offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through CyberScout, a TransUnion Company, to individuals to help protect their information. Additionally, MCSE 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

MCSE remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at jennifer.stegmaier@wilsonelser.com or 312-821-6167.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Jennifer S. Stegmaier

EXHIBIT A