To our Parents and Guardians:

We regret to inform you that on January 7th, we were notified by PowerSchool that, “On December 28, 2024, PowerSchool became aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals”. Later, on January 8th through communication with PowerSchool, other local school communities, cyber security communities, and our own internal investigations we learned that ***<u>Merrimack Student and Staff data was accessed and copied to an unauthorized source</u>***. We also found that this occurred to PowerSchool customers globally, not just Merrimack. PowerSchool claims that the data was found and securely destroyed. We will be in close contact with PowerSchool and will keep you updated as we receive new information from them.

Here is the timeline of events as we understand them today:

- On or about Dec 19, compromised credentials of a PowerSchool employee were used to gain access to PowerSchool community-focused customer support portals, PowerSource.

- On Dec 22, the compromised credential was used to gain access to many PowerSchool SIS instances.

- PowerSchool was notified by the unauthorized party of the credential compromise and the unauthorized taking of data on Dec. 28. PowerSchool then immediately hired a third-party cybersecurity advisor to assist.

- PowerSchool notified the District on Jan 7 stating, “On December 28, 2024, PowerSchool became aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals” and that they will be releasing more information through a webinar on January 8th.

- January 8th PowerSchool notified us through the webinar that the content of the copied data was the Student and Staff data tables. Merrimack School District ***<u>does not</u>*** populate all information in these tables, such as Social Security numbers; however, ***<u>we do populate</u>*** information like grades, street addresses, phone numbers, parent/guardian names, and in some instances, medical data like doctor names, doctor phone numbers, and brief medical notes in these tables.

- PowerSchool also claims, “We have taken all appropriate steps to prevent the data involved from further unauthorized access or misuse. We do not anticipate the data being shared or made public, and we believe it has been deleted without any further replication or dissemination.”

- January 8th we completed our own investigation using the indicators of compromise given to us at the time and verified that on Dec 22 our PowerSchool instance was accessed, data was taken.

We are taking this matter extremely seriously. We share your deep concern about unauthorized access to confidential information about students and staff. We are further upset by PowerSchool's unacceptable 10-day delay in notifying us about the breach.

We are committed to ensuring that protecting student and educator data remains secure. We are in contact with the company, and in the interest of transparency, we will provide updates as new information becomes available.

Thank you for your patience and understanding as we navigate this situation. Please email databreach@sau26.org if you have any questions or concerns.