Dear Valued Customer,

As a main point of contact for your school district, we are reaching out to make you aware 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, PowerSource. Your organization's Technical Contact was informed of this incident earlier today. Over the succeeding days, our investigation determined that an unauthorized party gained access to certain PowerSchool SIS customer data using a compromised credential.

However, our thorough forensic investigation has confirmed that information related to other PowerSchool products you have were not affected as a result of this incident. Please note there is no further action needed from you at this time relative to your non-PowerSchool SIS products, and we are simply notifying you to be as transparent as possible and because we value our partnership with you. We have already notified technical contacts responsible for PowerSchool SIS in your organization.

As soon as we learned of the incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. We have also informed law enforcement.

We have also deactivated the compromised credential and restricted all access to the affected portal. Lastly, we have conducted a full password reset and further tightened password and access control for all PowerSource customer support portal accounts.

Importantly, the incident is contained, and we have no evidence of malware of continued unauthorized activity in the PowerSchool environment. PowerSchool is not experiencing, nor expects to experience any operational disruption and continues to provide services as normal to our customers.

We are addressing the situation in an organized and thorough manner, following all of our incident response protocols. PowerSchool is committed to providing affected customers with the resources and support they may need as we work through this together.

Again, although your product was not impacted, we wanted to assure you that we are addressing the situation in an organized and thorough manner following all of our incident response protocols. Should you have any questions, please do not hesitate to contact your customer service manager. Thank you for your continued support and partnership.

Best,
Hardeep Gulati
Chief Executive Officer

Paul Brook
Chief Customer Officer

cc: **Mishka McCowan**
Chief Information Security Officer