

From: [Lance Harrison](#)
To: [Consumer Protection Mailbox](#)
Cc: [James Simeri](#)
Subject: PowerSchool Security Incident
Date: Monday, January 13, 2025 5:39:10 PM

Some people who received this message don't often get email from lance.harrison@psd201.org. [Learn why this is important](#)

Dear Office of Attorney General,

During the week of January 7, 2025, PowerSchool informed all their customers of the cybersecurity incident throughout the nation involving unauthorized access to certain PowerSchool Student Information System (SIS) data. Preston School District (PSD) uses PowerSchool in its operations to manage school data and student educational records.

Since that initial message, PowerSchool has now confirmed that the breach contained information from some of Preston School District's families and educators, although we do not yet know which individuals were impacted or the specific data included in the breach. As such, per Idaho Code §28-51-105(1), we are notifying the Attorney General's Office of the security breach that affected some of our staff and/or students. In compliance with the Student Data Privacy & Security Policy, I also notified the Executive Director of the State Board of Education and the State Superintendent of Public Instruction of this PowerSchool data breach. Additionally, we sent an email to Preston School District staff, students, and parents about the data breach.

PowerSchool indicated that the data taken from their portal primarily includes teacher, parent, and student contact information with data elements such as name and address. They have determined that for a certain portion of individuals across their customer base, some personally identifiable information (PII), such as social security numbers (SSN), may be impacted. They are working with urgency to complete their investigation and determine whether PII belonging to students or teachers in PSD was included.

PowerSchool reported that their cross-functional cybersecurity response team with third-party experts, has contained the incident, and they have no evidence of malware or continued unauthorized activity in the PowerSchool environment. PowerSchool added that they have taken all appropriate steps to prevent the data involved from further unauthorized access or misuse. PowerSchool does not anticipate the data being shared or made public, and they believe it has been deleted without any further replication or dissemination.

The incident was isolated to an outside PowerSchool platform. District servers and systems were not breached. At the first of this school year when the district transitioned to a new firewall, Preston's IT Director updated the list of IP addresses blocked, many from countries

where cyber-attacks often originate. Furthermore, Preston School District has previously adopted and posted policies based on the model policy developed by the Board of Education related to student data privacy & security (PSD Policy 681.5) and student records (PSD Policy 680).

As we determine the scope of the impact and the nature of the compromised data, updated information will be communicated to individuals who have been affected. Additionally, in the coming days, PowerSchool will be providing more information and resources, including identity protection services or credit monitoring. If applicable, this information will also be provided to staff, students, and parents as it becomes available from PowerSchool.

Protecting our students and teachers is important to us.

Respectfully,
Lance Harrison

Lance K. Harrison, PhD
Superintendent of Schools
Preston School District #201
105 E 2nd S
Preston, ID 83263
(208) 852-0283