NORTH CAROLINA
DEPARTMENT OF PUBLIC INSTRUCTION

PowerSchool Cybersecurity Incident Updates: Credit Monitoring and More

Dear District and School Leaders,

We are reaching out to provide you with the latest updates on the PowerSchool cybersecurity incident and the ongoing efforts to support impacted students, educators and families. This message includes key details on the next steps, resources and how you can assist your community in navigating the situation.

In addition, we are sharing all known information on the incident at the request of several public school units (PSUs)

Latest Update from PowerSchool (1/29/25):

This afternoon, PowerSchool shared that they had begun the process of filing state attorneys general notifications across applicable U.S. jurisdictions on behalf of its customers.

In the coming days, PowerSchool will begin providing formal legal notice of the cybersecurity incident to current and former students (or their parents/guardians as applicable) and educators whose information was determined to be involved.

In addition, a direct email notification will be distributed by Experian on behalf of PowerSchool in the coming weeks to applicable current and former students (or their parents/guardians as applicable) and educators for whom we have sufficient contact information. PowerSchool will also launch a website and distribute a media release to ensure they reach as many involved individuals as possible and provide them with resources to protect their information.

These notices will include instructions for involved individuals on how to enroll in the credit monitoring and

identity protection services that are being offered by PowerSchool.

Overview of the PowerSchool Data Breach

On the afternoon of January 7, 2025, PowerSchool notified the North Carolina Department of Public Instruction (NCDPI) and North Carolina public schools about a cybersecurity incident that impacted student and teacher/staff data across their global client base via the PowerSchool Student Information System (SIS). This incident was not isolated to North Carolina.

NCDPI received copies of the audit logs from PowerSchool and worked with the North Carolina Local Government Information Systems Association (NCLGISA) Strike Team. This review CONFIRMED that all NC PSUs that ever used PowerSchool were impacted by this cybersecurity breach, including the PSUs that migrated to Infinite Campus in phase 1.

The incident occurred when a PowerSchool contracted employee's credentials were compromised via malware allowing unauthorized access to an administrative maintenance tunnel. The threat actor used the maintenance tunnel to export the STUDENT and TEACHER table from each PSU instance.

PowerSchool has shared that all impacted data has been contained and destroyed. PowerSchool is working alongside law enforcement to monitor the dark web for any activity involving exposed data.

PowerSchool confirmed there were no actions any PSU or NCDPI could have taken to prevent this cybersecurity incident.

In North Carolina, 910 student records involved in this incident included Social Security Numbers (SSNs). There were approximately 312,000 staff and teacher records that also included SSNs. NCDPI has shared a spreadsheet with each PSU that includes the number of records breached and the types of data that might include Personally Identifiable Information (PII).

PowerSchool will conduct all necessary notifications once all analysis is completed to ensure appropriate and accurate compliance with local, state and federal requirements and laws. PowerSchool will also offer two years of Identity protection for staff and students and two years of credit monitoring for adults from Experian. This offer is for all impacted individuals whose data was included in this breach regardless of what personal data was included. PowerSchool will proved the website URLs to those impacted when it becomes available.

Powerschool will share the links for Identity protection and Credit Monitoring as they become available. These links should be shared with the PSU community via websites, communications and other appropriate methods.