STILLWATER AREA PUBLIC SCHOOLS

Minn. Stat. § 13.055, subd. 2(b) Investigation Report
"PowerSchool Student Information System Cyber Incident"

April 22, 2025

The data in this report is **public** under Minnesota Statutes, §13.02, subdivision 19, and Minnesota Statutes, §13.43, subdivision 2(a)(5).

This report is prepared in accordance with Minnesota Statutes, §13.055, which requires government entities to notify individuals in the event of a data breach and to prepare a report describing the facts and results of the investigation.

This document serves both as:

- The required notice to affected individuals under Minn. Stat. §13.055, and
- The formal investigation report under Minn. Stat. §13.055, subd. 2(b).

Minnesota Statutes, section 13.055, subdivision 2(b), requires government entities, including Stillwater Area Public Schools (the "District"), to "prepare a report on the facts and results of the investigation" into "any breach in the security of data." This report includes the following information:

1. *"a description of the type of data that were accessed or acquired";*
2. *"the number of individuals whose data was improperly accessed or acquired";*
3. *"if there has been final disposition of disciplinary action for purposes of Minn. Stat §13.43, the name of the employee determined to be responsible for the unauthorized access or acquisition, unless the employee was performing duties under Minn. Stat CH. 5B; and*
4. *"the final disposition of any disciplinary action taken against each employee in response".*

I. A description of the type of data that were accessed or acquired

On January 7, 2025, PowerSchool, the District's Student Information System (SIS) provider, informed Stillwater Area Public Schools of a cybersecurity incident involving unauthorized access to SIS environments hosted by a third-party vendor. Stillwater communicated with families beginning on January 9, 2025. This incident was part of a broader attack that affected multiple school districts utilizing the PowerSchool SIS.

According to PowerSchool's investigation, an unauthorized actor gained access between December 19, 2024 and December 23, 2024, using compromised login credentials from PowerSource, PowerSchool's support portal. These credentials were used to access certain SIS environments, including the one used by Stillwater Area Public Schools. The attacker exfiltrated specific data tables, including those containing student and staff information. This access was not a result of any actions or vulnerabilities within Stillwater's internal systems.

PowerSchool detected the unusual activity through its internal security monitoring tools and quickly initiated its incident response protocols. The compromised accounts were disabled, and PowerSchool worked with leading cybersecurity firm CrowdStrike to conduct a forensic investigation. CrowdStrike's final report confirmed that the attacker had access to and exported

specific datasets but subsequently deleted the stolen data during their interaction with PowerSchool.

Stillwater Area Public Schools was not directly targeted in this incident but was impacted due to the nature of the shared hosting environment. As soon as the District was made aware of the situation on January 7, 2025, it initiated its own cybersecurity response plan, employed an external cyber security firm, began reviewing impacted data, and collaborated with PowerSchool to notify affected individuals. There is no evidence at this time that any of the accessed information has been misused or publicly released.

Types of Data Accessed:

A. Student Information: Names, addresses, dates of birth, emergency contacts, homeroom teachers, enrollment dates, guardian phone numbers, and some individual emergency contacts.
B. Staff Information: Names, district email addresses, and district phone numbers.

No financial information or Social Security numbers were accessed, as this information is not stored in PowerSchool.

Measures Taken:

C. PowerSchool has taken the following steps in response to the incident:
    a. Deactivated compromised credentials and restricted access to the support portal.
    b. Conducted a full forensic investigation and published a summary of findings.
    c. Implemented biometric authentication for employees and limited maintenance access windows.
D. Stillwater Area Public Schools has:
    a. Maintained communication with PowerSchool to monitor developments.
    b. Notified staff and families through email and its website.
    c. Participated in cross-district collaboration on cybersecurity response practices.

II. The number of individuals whose data was improperly accessed or acquired

Stillwater Area Public School's investigation determined that data from approximately 19,286 records belonging to students enrolled at Stillwater Area Public Schools between 2020 and 2024 was improperly accessed.

III. If there has been a final disposition of disciplinary action for purposes of Minn. Stat §13.43, the name of each employee determined to be responsible for the unauthorized access or acquisition

No Stillwater Area Public Schools employee was found to be responsible for the unauthorized access. The incident was the result of compromised credentials used against PowerSchool's third-party systems. As such, no disciplinary action was taken against District staff.

IV. The final disposition of any disciplinary action taken against each employee in response.

Not applicable. No disciplinary action was taken against any Stillwater Area Public Schools employee in connection with this incident.

Learn more about this incident at
stillwaterschools.org/our-district/cybersecurity-incident

Questions can be directed to Stillwater Area Public Schools at comments@stillwaterschools.org or to PowerSchool directly at 833-918-9464
