THE VIRGIN ISLANDS DEPARTMENT OF
EDUCATION

Office of Public Relations
Telephone: 340.774.0100 (STT/STJ) 340.773.1095 (STX)

FOR IMMEDIATE RELEASE **0102-25**
January 10, 2025

For More Information Contact:
Shayla S. Solomon
Director, Public Relations & Communications shayla.solomon@vide.vi
www.vide.vi ~ www.facebook.com/usvi.vide

Virgin Islands Department of Education Informs Public of Nationwide PowerSchool Data Breach

The Virgin Islands Department of Education (VIDE) has been informed by PowerSchool, the nation's largest provider of cloud-based education software for K-12 schools, of a nationwide data breach impacting school districts across the country. This breach has affected personal information of students and educators, including data from public and private schools that utilize PowerSchool's systems to manage information such as enrollment, grades, records, attendance, etc.

The incident occurred off-site at PowerSchool's facilities and VIDE wants to reassure its parents, students, faculty, and all stakeholders that no actions by the Department or individual schools contributed to this breach. This was an international cyberattack targeting PowerSchool's customer support portal. According to PowerSchool's statement, the breach was discovered on December 28, 2024, and involved a compromised credential allowing unauthorized access to certain data. PowerSchool has since taken steps to contain the incident and prevent further unauthorized use of the data.

Scope of the Breach: PowerSchool representatives have reported that an export data manager tool was used to extract student and teacher tables. These tables primarily include contact information, such as names and addresses. In some cases, data may also include Social Security Numbers (SSNs), medical records, and grades for current and former students. Importantly, no bank account or credit card information is stored within PowerSchool's systems and, therefore, was not affected.

PowerSchool's Response: PowerSchool has stated that the data breach is contained and that they believe the data will not be shared publicly. The company has paid an undisclosed amount to the perpetrator in exchange for evidence that the data was destroyed. PowerSchool continues to monitor the dark web to ensure no additional copies of the data are circulating. Furthermore, they have indicated that no other PowerSchool products were compromised, and the incident has not disrupted their services.

VIDE's Commitment to Transparency: The VIDE is actively sharing updates provided by PowerSchool and will continue to keep its stakeholders informed as more information becomes available.

For further clarity, **a special live presentation for parents is scheduled for Monday, January 13, 2025, from 6:00 p.m. to 7:00 p.m**. VIDE representatives will explain the breach, its containment, and its impact on data privacy.

Presentation Details: Join the live presentations using the following login information (link or QR Code):

http://bit.ly/3Pxy8m6

VIDE’s Data Safeguards: Although this incident occurred off-site, the VIDE remains committed to ensuring the privacy and security of stakeholder information and has implemented robust internal safeguards, including:

- Multifactor Authentication (MFA): Enabled in 2024 to prevent unauthorized access.
- Access Control Policies: Employing segregation of duties and least privilege principles to limit data access.
- Antivirus and Anti-Malware Protection: Continuous monitoring for vulnerabilities and suspicious activity.
- Firewalls and Network Segmentation: Which ensures isolation of systems and departmental data.

VIDE emphasizes that these measures remain effective in safeguarding data managed locally within the Department.

Assurance to the Community: The VIDE takes this situation very seriously and assures the public that it is working diligently with PowerSchool as they work with other national agencies to investigate and mitigate the breach. While this was a global incident beyond the control of individual districts, the Department remains proactive in providing updates and support to students, parents, and staff.

PowerSchool officials have stated, “All appropriate steps have been taken to ensure the data involved is protected from further misuse, and there is no evidence of malware or ongoing unauthorized activity.” PowerSchool has also confirmed that it continues to provide uninterrupted services to its customers.

Disclaimer: Some language in this press release is directly cited from statements issued by PowerSchool. For further information on their official updates, visit https://www.powerschool.com/

###