February 20, 2025 - Northport Public School is actively monitoring a recent cybersecurity incident that impacted PowerSchool, a company that provides Northport Public School with student information management software.

Specifically, we recently learned that on December 28, 2024, PowerSchool discovered that an unauthorized actor gained access to certain customer data, potentially including some information relating to Northport Public School. At this time, broadly speaking, our understanding is that the elements of information involved in this incident generally may include the following: names, contact information, dates of birth, Social Security numbers, medical alert information, and other related information.

We understand that on or about January 29, 2025, PowerSchool began sending notifications via email directly to certain impacted individuals and families to notify them of the incident. It is anticipated that these incident notification emails from PowerSchool will be sent to affected individuals and families on a rolling basis in the coming days and weeks. As of January 29, 2025, PowerSchool has represented its investigation into the incident has not yet concluded. As such, our understanding of the scope of the incident is actively evolving and there remains a possibility that those families who have not yet received an email from PowerSchool may receive one in the future, along with further communication from Northport Public School.

While we await final findings from PowerSchool concerning the scope of the impact of this incident, it is important to remain diligent in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

PowerSchool is offering two years of complimentary identity protection services to students and educators whose information was involved. For adult students and educators, this offer will also include two years of complimentary credit monitoring services. If you are interested in enrolling, please sign up via one of the two following options:

Option 1 from PowerSchool: If the Involved Individual is 18 or Over

- Ensure that you enroll by May 30, 2025 (Your code will not work after this date at 5:59 UTC)
- Visit the Experian IdentityWorks website to enroll: http://www.experianidworks.com/plus
- Provide your activation code: CTYU949PRK
- For over the phone assistance with enrollment or questions about the product, please contact Experian's customer care team at 833-918-9464
- Be prepared to provide engagement number: B138812
- Experian's call center hours are Monday through Friday, 8:00am through 8:00pm Central Time (excluding major US holidays.)

Option 2 from PowerSchool: If the Involved Individual is Under 18

- Ensure that you enroll by May 30, 2025 (Your code will not work after this date at 5:59 UTC)
- Visit the Experian IdentityWorks website to enroll: Enroll Now
- Provide your activation code: CEBP456TRK
- For over the phone assistance with enrollment or questions about the product, please contact Experian's customer care team at 833-918-9464
- Be prepared to provide engagement number: B138813

Further, PowerSchool has set up a dedicated response line for this incident. The response line is available Monday through Friday, 8:00 am to 8:00 pm Central Time. You may contact PowerSchool's response line directly at (833) 918-9464. Additionally, PowerSchool has published additional information on its website, which is available at: https://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/

We acknowledge this may be concerning news. As always, our #1 priority is to ensure the safety and security of our students, staff and community. We will share further updates as relevant information becomes available.

Sincerely,
Northport Public School

- OTHER IMPORTANT INFORMATION -

1. Placing a Fraud Alert on Your Credit File.

You may place an initial one-year "fraud alert" on your or your student's credit files (if one exists), at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your or your student's credit file, at no charge (to the extent one exists). A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and

following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ (800) 349-9960 (888) 298-0045	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze (888) 397-3742	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 https://www.transunion.com/credit-freeze (888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report (to the extent one exists) every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

5. Protecting Your Medical Information.

The following practices can provide additional safeguards to protect against medical identity theft:

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.