

May 20, 2022

Dear Parent or Guardian of [STUDENTNAME]:

Chicago Public Schools was recently made aware of a data security incident involving one of our vendors that may have impacted your child, [STUDENTNAME], and their personal information between 2015 and 2019. This letter contains information about the incident, our response, steps to safeguard your child's information, and safety measures that have been put in place to assure the security of information in the future. At this time, there is no evidence to suggest that this data has been misused or distributed.

A technology vendor for CPS called Battelle for Kids recently notified CPS that on December 1, 2021, Battelle for Kids was the victim of a ransomware attack on a server used to store CPS student information for school years 2015-2016, 2016-2017, 2017-2018 and 2018-2019. Battelle for Kids is a nonprofit technology organization that stores student course information and assessment data for the purposes of teacher evaluations.

Specifically, an unauthorized party gained access to your child's name, date of birth, gender, grade level, school, Chicago Public Schools student ID number, State Student ID number, information about the courses your student took, and scores from performance tasks used for teacher evaluations during school years 2015-2016, 2016-2017, 2017-2018 and/or 2018-2019. The server did not store any other information about your child. **No Social Security numbers, no financial information, no health data, no current course or schedule information, and no course grades or standardized test scores were involved in this incident.**

This incident has been reported to and investigated by the appropriate law enforcement authorities, including the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS). Battelle for Kids is currently monitoring and will continue to monitor the internet in case the data is posted or distributed. **We can report that as of this time, there is no evidence to suggest that this data has been misused, posted, or distributed.** According to data security experts, including law enforcement, the lack of financial information contained in the data decreases the likelihood that the data will be misused.

Although the data that was inappropriately accessed did not include any financial information or your child's Social Security number, we know that you may be concerned about fraudulent activity on your child's behalf.

Out of an abundance of caution, CPS is providing free credit monitoring and identity theft protection for any student who was impacted. The coverage includes twelve months of credit monitoring, twelve months of access to an identity restoration program that provides assistance in the event that your child's identity is compromised, and up to \$1,000,000 in identity theft insurance with no deductible. Your child's unique access code for this coverage is [NUMBER]. To enroll, please visit <https://response.idx.us/cps> or call the toll-free hotline at 833-909-4007.

You can also access a free credit report for your child through annualcreditreport.com, a free resource authorized by the federal government. Additionally, the following credit reporting agencies offer a free service allowing you to receive fraud alerts and to freeze access to your child's credit if necessary:

- Experian - <https://www.experian.com/fraud/center.html>, or 1-888-397-3742, or P.O. Box 2002, Allen, TX 75013.
- TransUnion - <https://www.transunion.com/fraud-victim-resources>, or 1-833-395-6938, P.O. Box 2000, Chester, PA 19022.
- Equifax - <https://www.equifax.com>, or 1-888-378-4329, or P.O. Box 740241, Atlanta, GA 30374.

We also encourage you to visit the Federal Trade Commission (FTC) website at <https://www.identitytheft.gov/#/Info-Lost-or-Stolen> for more information about fraud alerts and security freezes from consumer reporting agencies. You may also contact the FTC at 1-800-FTC-HELP (1-800-382-4357).

Should you have additional questions regarding the incident, please contact 833-909-4007 or email BFK-Breach-Info@cps.edu. If you have received this email, it means your child, [STUDENTNAME], was impacted.

Although CPS did not cause this incident, we are deeply committed to the security of student information, and we expect the same level of care and commitment from our vendors. Battelle for Kids has informed CPS that they have taken several mitigation measures to reduce the risk of this type of incident occurring in the future, including a plan for the timely and secure deletion of outdated data, migration to enterprise cloud services, enhanced network security, and the retention of a third-party security firm for up-to-date defenses and industry-leading practices for the ever-evolving needs of cybersecurity.

Please know that the protection of your child's personal information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause you.

Please visit cps.edu/databreach for more information, including answers to Frequently Asked Questions about this incident. This letter is available in multiple languages on our website.

Sincerely,

Edward Wagner
Acting Chief Information Officer
Chicago Public Schools