PEARSON DATA INCIDENT FAQ

Was Indian Prairie School District the only school district impacted by this incident?
No. A total of 13,000 Pearson school district and university clients were impacted across the country.

Did the Pearson data incident occur on a District 204 server?
No. Pearson Clinical Assessment experienced a data security incident related to their AIMSweb 1.0 product by an unauthorized third party accessing a Pearson server. No District 204 servers were compromised or involved in this incident.

Why should I consider signing up my child for free identity theft and credit monitoring provided by Pearson when they don't have a credit file yet?
According to Pearson, the student information obtained during this incident is limited to student first name and last name, and in some cases date of birth. No other identifying information was obtained. Pearson does not maintain any social security numbers or any financial information. In an abundance of caution, Pearson is providing free identity theft and credit monitoring protection through Experian. According to Experian, they "do not knowingly maintain credit reports on minor children. However, it is not uncommon for a parent to add a child as an authorized user or joint account holder, in which case they may have a legitimate credit history." If you have any concerns that someone may try to use your child's information, you can sign up for free identity theft and monitoring services using the following instructions: http://ipsdweb.ipsd.org/newsfiles/news_104263_1.pdf.

How does the District protect student and staff data?
As a school district, we take very seriously the security of all student, family and staff data. Only the most limited data is provided to vendors for required services. Contracts with outside vendors are closely vetted to ensure measures are in place at all times to safeguard that data. The District implements data privacy agreements with each of our third-party vendors to establish operating requirements to protect District data. These include provisions for compliance with state and federal laws, safeguards and requirements for the protection of the privacy, confidentiality and integrity of District data, protocols in the event of a data incident, as well as identifying the prohibited uses of data. In addition to written contractual agreements, the District has best-practice-focused security protocols, adaptive and AI-based monitoring tools and proactive interventions established that are focused on the protection of District data.

Who can I contact if I have additional questions?
Pearson Clinical Assessment has a dedicated email for responding to questions or concerns related to its data incident. You can email Pearson at aimsweb1request@pearson.com.