

Suggested Subject Line of Email: Aeries Data Security Incident

May 12, 2020

Dear Rocklin Unified School District Families,

This letter is to inform you of a data security breach that impacted Aeries®, the District's Student Information System (SIS) which stores and provides access to certain student and parent information for Rocklin Unified School District. We are one of hundreds of districts using Aeries® SIS that was affected by this breach. RUSD has been a customer of Aeries® for over 20 years, and in that time has had no unauthorized access or data breaches with this software. We do not believe there is any reason to be alarmed or unduly concerned, but we wanted you to be informed about what happened.

Timeline with information provided to us from Aeries:

On April 27, 2020 we were informed there may have been unauthorized access to the Aeries® SIS on November 4th, 2019. The [initial report](#) was focused on Aeries Hosted Databases, which we do not use. Our Student Information System is housed on our own servers here in Rocklin.

On May 6, 2020 we learned that it may have also affected on-premise databases similar to ours. Following directions provided by Aeries, we immediately contacted Aeries and got confirmation on May 11, 2020 that our data was also accessed.

This breach may have revealed **Parent and Student Login information, physical residence addresses, email addresses, and encrypted passwords**. However, no other data elements were impacted as a result of this incident. Social security numbers, credit card data, or other personal information *is not* kept in our Aeries database.

With access to encrypted passwords, unauthorized people may be able to deconstruct weak, common or simple passwords and subsequently enable unauthorized access to parent and student Accounts and data stored in the Aeries® SIS.

We have been informed that local and federal law enforcement officials were notified of the incident, charges were filed and the people responsible were arrested. The investigation of their misconduct is continuing.

While there is no evidence to suggest that your specific data was misused, out of an abundance of caution, we will reset the account passwords for all parents and students beginning Tuesday May 12, 2020. *To reset your password, please follow the 'Forgot Password' link on the Aeries Parent/Student Portal.*

Further, we will be enforcing stricter password security guidelines as an added precaution against the possibility of future such incidents. All new passwords will employ the following guidelines:

- *Force Users to Change Passwords Every 6 months (minimum)*
- *Days Prior to Expiration to Notify Users - 10 days (minimum)*
- *Minimum Length: 8-16 Characters*

- *Require a Special Character*
- *Require Letters and Numbers*
- *Require Upper and Lower case*

We have no reason to believe that any data was accessed revealing sensitive information such as, Social Security numbers, credit card numbers, financial account information, or other information directly impacting your credit rating. Rocklin Unified School District *does not* keep this type of information associated with your Aeries account. Nevertheless, If you suspect your personal information has been misused, visit the Federal Trade Commission's site at [IdentityTheft.gov](https://www.ftc.gov/identitytheft) to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcement for their investigations.

For links and more information go to www.rocklinusd.org/databreach. Here you will also see what actions Aeries is taking to prevent this from happening to our school district and others in the future. If you have any questions, including how to reset your password, please email safedata@rocklinusd.org and one of our RUSD Technology Services experts will respond and help you in a timely manner.

Thank you,

Rocklin Unified School District