Email Subject: Aeries Security Breach

Dear Charter Alternative Program Parents,

This letter is to inform you of a data security incident that impacted the Aeries® Student Information System which stores and provides access to certain student and parent information for schools across the United States. While we do not believe there is any reason to be concerned, we wanted you to be informed about what happened.

On May 6th, 2020, we were informed that there may have been unauthorized access to the Aeries® SIS on November 4th, 2019 which may have revealed Parent and Student Login information, physical residence addresses, emails addresses, and password hashes. Even though a password hash is an encrypted password (not visible), unauthorized persons may be able to deconstruct weak, common or simple passwords, which would enable the person to access unauthorized Parent and Student Accounts and data stored in the Aeries® SIS. Based on the report we received from Aeries, no other data stored in our AERIES database was affected, including grades, credits, & transcripts.

We have been informed that local and federal law enforcement officials were notified of the incident, charges were filed on a single individual, and the investigation is continuing.
While there is no evidence to suggest that data was misused, we will be resetting the account passwords for all Charter parents out of an abundance of caution tomorrow, May 19th.
As an added precaution against the possibility of future such incidents, we will be enforcing stricter password security guidelines, which will require the following:

- Minimum Length: 8 Characters
- Require a Special Character
- Require Letters and Numbers
- Require Upper and Lower case

Upon being made aware of the incident, Aeries Software took action to ensure the security of the system and has taken additional technical measures to prevent future incidents, including adopting new security protocols. We will continue to work closely with Aeries Software to ensure that your data remains as secure as possible. If you suspect your personal information has been misused, you can visit the FTC's site at IdentityTheft.gov to get further information. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.