Aeries Software, Inc.

Date: April 27, 2020

NOTICE OF DATA BREACH

Dear Hosted Customer:

We are contacting you about a data security incident that may have affected the Aeries Student Information System.

What Happened?	The purpose of this notice is to inform you that your database may have been subject to unauthorized access involving your Parent and Student Data. In late November 2019, Aeries Software became aware of unauthorized attempts to access data through the Aeries SIS. In response, we immediately began an investigation into whether these attempts had been successful and, if so, how they had been accomplished, what impact, if any, they may have had on data, and what steps we could take to thwart future unauthorized access to data through the Aeries SIS using the same or similar means. At the time, internal investigation did not reveal any compromise of the Aeries SIS or data. Nevertheless, Aeries Software deployed a series of security patches in the December 20, 2019 version of the Aeries SIS which addressed the results of our internal investigation. Then, in late January 2020, we were informed by a locally hosted District that their database may have been previously subject to unauthorized access, they had informed local authorities, and a criminal investigation was underway. We now understand that the investigation by the authorities is ongoing and we are working closely with local law enforcement and federal authorities as well as the District to determine what transpired, by whom it was perpetrated, and what impact, if any, it may have had on data. In working with the District and law enforcement officials, in March 2020 we were able to expand our earlier investigation with the new information as to the methods used by the individuals who had accessed data without authorization. Specifically, we determined that the unauthorized access had included Parent and Student Login information, physical residence addresses, emails, and “password hashes.” With access to a password hash, weak, common or simple passwords, can be deconstructed to gain unauthorized access to Parent and Student Accounts. According to the results of our investigation, there is evidence to suggest that your database in our Hosted environment may have been subject to unauthorized access by this means. However, we understand the perpetrators have been taken into custody and the unauthorized access has been terminated.
What Information Was Involved?	At the moment, our investigation has revealed Parent and Student Login information, physical addresses, emails, and passwords hashes have been subject to unauthorized access.

What We Are Doing	While there is no evidence to suggest that your data was misused, Aeries Software policy requires that we notify our customers whose data may have been subject to unauthorized access. Out of an abundance of caution, we strongly recommend that you reset the account passwords for your parents and students as soon as possible. To assist our customers with Password security, in the March 26th version of Aeries, a new feature was released to provide System Administrators the ability to run a process that resets the passwords for Parents and/or Students in the **PWA** table and sends an email that includes a link for that account to reset their password. We strongly recommend ensuring all passwords meet parameters which reflect industry security best practices, such as: *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* Aeries documentation can be found here: Aeries Password Requirements It is also important to understand that upon being made aware of these vulnerabilities, we took immediate action to ensure that critical patches were deployed to ensure that the vulnerabilities were no longer a threat to the system. In addition, we have taken additional technical measures to prevent future incidents and we are adopting new security protocols to increase protection of all customer data. In addition to allocating several resources to perform a rigorous internal security audit, we will also be engaging an independent third party to assist us in conducting a complete audit and analysis of our system security.
What You Can Do	While our password guidelines are optional, we strongly recommend ensuring all passwords meet parameters which reflect industry security best practices, such as: *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* For more information on password settings, the documentation can be found here: Aeries Password Requirements. Documentation for the new Reset Parent/Student accounts can be found here: Reset Parent/Student Account Passwords. There is nothing to suggest that any data was accessed revealing Social Security numbers, credit card numbers, financial account information, or other information directly impacting your credit rating. Nevertheless, If you suspect your personal information has been misused, visit the FTC's site at IdentityTheft.gov 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 enforcers for their investigations. In addition, you can contact all three major credit bureaus to request that your credit reports be sent to you, free of charge, for your review. 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. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

For More Information	We will continue to follow-up with any additional recommendations, details, or bulletins that you should be made aware of as more information comes in. For more information, please email legal@aeries.com.