Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>

Aeries Software, Inc. ("Aeries"), which provides the Aeries® Student Information System to San Dieguito Union High School District ("San Dieguito"), is writing to inform you of a security event. This letter includes information about the event and steps you may take to better protect yourself, should you feel it necessary. Please know that we recognize the trust you place in Aeries and San Dieguito to protect your information, and we sincerely regret any inconvenience or concern this incident may have caused you.

What Happened? On January 28th, 2020, San Dieguito alerted Aeries that their database may have been potentially subject to unauthorized access. We immediately launched an investigation into the nature and scope of the incident and took measures to secure the database. We also assisted San Dieguito and its forensic experts with their investigation into the incident. On February 25, 2020, the forensic investigations revealed that San Dieguito's Aeries database was subject to unauthorized access from April 2019 to January 2020. San Dieguito undertook a labor-intensive review of the affected database to determine the scope of personal information contained within. San Dieguito has asked Aeries to notify you out of an abundance of caution because your information was present in the affected database.

What Information Was Involved? While the investigations were unable to confirm whether your information was actually viewed by the unauthorized individual(s), the investigations confirmed that the following information related to you was present in the affected database: <<Breached Elements>>.

What We Are Doing. We take this incident and the security of personal information very seriously. Upon discovery of this incident, we immediately took steps to secure the database and prevent further access. As part of Aeries's ongoing commitment to privacy, we reviewed our existing policies and procedures and implemented additional safeguards to further secure the information in our systems. Aeries is also cooperating with local authorities and the FBI, who have launched an investigation and have identified two U.S. individuals who are suspected of causing this incident.

What You Can Do. Aeries encourages you to remain vigilant against incidents of identity theft and fraud, review your account statements and monitor your credit reports for suspicious activity. Please review the enclosed *Steps You Can Take to Protect Your Personal Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line that we have established at 855-913-0609, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, Monday through Friday, excluding U.S. holidays.

Sincerely,

Jonathan Cotton
Executive Director of Operations
Aeries Software, Inc.

Steps You Can Take to Protect Your Personal Information

You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with
Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf),
Experian (https://www.experian.com/fraud/center.html), or
Transunion (https://www.transunion.com/fraud-victim-resource/place-fraud-alert).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

More information can also be obtained by contacting the Identity Theft Clearinghouse at the Federal Trade Commission listed above.