

1 Daniel L. Warshaw (CA Bar No. 185365)
2 **PEARSON, SIMON & WARSHAW, LLP**
3 15165 Ventura Boulevard, Suite 400
4 Sherman Oaks, CA 91403
5 Telephone: (818) 788-8300
6 Facsimile: (818) 788-8104
7 Email: dwarshaw@pswlaw.com

8 *Attorneys for Plaintiffs and the Proposed Class*
9 *(Additional Counsel on Signature Page)*

10 **UNITED STATES DISTRICT COURT**
11 **CENTRAL DISTRICT OF CALIFORNIA**
12 **WESTERN DIVISION**

13 **ANURAG GUPTA and by and**
14 **through him, D.G. and V.G., his**
15 **minor children,**
16 *individually and on behalf of all others*
17 *similarly situated,*

18 **Plaintiffs,**

19 **v.**

20 **AERIES SOFTWARE, INC.,**

21 **Defendant.**

Case No. 8:20-cv-00995-FMO-ADS

CLASS ACTION

SECOND AMENDED CLASS
ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiffs Anurag Gupta and his minor children, D.G. and V.G. individually¹
 2 (“Individual Plaintiffs”) and Plaintiff Melinda Tomes (“Class Plaintiff”) on behalf of
 3 herself and all other persons similarly situated (collectively “Plaintiffs”), and through
 4 their attorneys of record, allege the following against Defendant Aeries Software, Inc.
 5 (“Aeries” or “Defendant”) based upon personal knowledge with respect to themselves,
 6 on information and belief derived from investigation of counsel, and review of public
 7 documents as to all other matters.

8 INTRODUCTION

9 1. Plaintiffs D.G. and V.G. are minor students at the ABC Unified School
 10 District (“ABC”) and Class Plaintiff Melinda Tomes is a parent of former students of
 11 the San Dieguito Union High School District (“SDUHSD”), which are two of many
 12 public school districts in California that utilize the Aeries School Information System
 13 offering (“Aeries SIS”) to manage student data. Unfortunately for Plaintiffs, Aeries did
 14 not adequately safeguard their data, and they and thousands of other students are now
 15 the victims of a large-scale, long-lasting data breach that will impact them for years to
 16 come. Individual Plaintiff Gupta is the natural parent of Individual Plaintiffs D.G. and
 17 V.G., and his data was also compromised in the same data breach. Class Plaintiff
 18 Tomes had her own Aeries account that was also compromised in the same data
 19 breach.

20 2. In November 2019, Aeries began internally investigating an attempt of
 21 unauthorized persons to access data through Aeries SIS.² According to Aeries, it did
 22 not discover any unauthorized access, but nevertheless, it updated the Aeries SIS on
 23 December 20, 2019, to fix security deficiencies it discovered during its internal
 24 investigation.

25
 26 ¹ Anurag Gupta and his minor children, D.G. and V.G. are bringing their claims on
 27 an individual capacity only and do not seek to represent the Class.

28 ² <http://aeries.com/notice-of-data-breach-4-27-2020> (last visited May 26, 2020)

1 3. In January 2020, Aeries learned that the local database of one of its school
2 district clients whose students' (as well as the students' parents' and guardians')
3 personal information was stored locally on the school districts' database and processed
4 through the Aeries SIS, was subjected to unauthorized access. Aeries undertook
5 another investigation.³

6 4. Aeries now admits that 166 databases hosted on Aeries servers and
7 storing data on behalf of the school districts (this Aeries server environment is referred
8 to herein as "Aeries Hosting") were subject to unauthorized access beginning on or
9 about November 4, 2019 (the "Data Breach"). According to Aeries, it did not discover
10 the unauthorized access of those Aeries Hosting databases until March 2020, and it
11 claims "the unauthorized access has been terminated."⁴ However, Aeries has not
12 disclosed when such access was terminated, and its assertion that it has resolved the
13 problem is doubtful given its inability to detect the intrusion for four months even
14 though it was on notice of intrusion attempts and known security deficiencies during
15 that time.

16 5. Despite having knowledge of the Data Breach as early as November
17 2019, and certainly no later than January 2020, Aeries did not notify its school district
18 customers of the Data Breach until April 27, 2020, when it issued a "Notice of Data
19 Breach" to school district customers.

20 6. The April 27, 2020 "Notice of Data Breach" disclosed only that the
21 following personal information was compromised: "Parent and Student Login
22 information, physical residence addresses, emails, and 'password hashes.'" Aeries
23 further acknowledged that "[w]ith access to a password hash, weak, common or simple
24
25

26 ³ *Id.*

27 ⁴ *Id.*

1 passwords, can be deconstructed to gain unauthorized access to Parent and Student
2 Accounts.”⁵

3 7. The Notice of Data Breach did not disclose that additional private
4 personal information was stored on behalf of its school district customers, including,
5 *inter alia*, (1) minor students’ immunization and other health records, (2) social security
6 numbers, (3) class grades, (4) standardized test information, (5) previous addresses,
7 and (6) parent’s or guardian’s credit or debit cards and other financial information used
8 to pay school fees and fines (collectively with the personal information identified in
9 paragraphs 6, 22, and 26, the “PII”).

10 8. More than two weeks after Aeries sent its school district customers the
11 Notice of Data Breach, ABC and SDUHSD finally provided notice of the breach to
12 parents and guardians of children attending their schools on about May 13, 2020,
13 including Mr. Gupta.⁶ This notice did not disclose any of the categories of students’,
14 parents’, or guardians’ PII that were compromised in the Data Breach. Nor did a
15 subsequent email sent on May 21, 2020, from ABC’s Director of Information and
16 Technology, which only provided instructions for how parents and students could
17 reset their passwords used to access Aeries SIS.⁷ On May 28, 2020, ABC finally sent a
18 more detailed notice with the subject line “An Announcement from Colin Sprigg.”⁸

19 9. SDUHSD also sent delayed notifications to parents and guardians of
20 children attending SDUHSD schools, including a press release dated May 14, 2020.⁹

21 10. Unfortunately, even Aeries’ subsequent investigations failed to uncover
22 that it was not only PII stored on Aeries Hosting that was compromised. In early May
23 2020, other school district customers discovered that PII processed through the Aeries

24 ⁵ *Id.*

25 ⁶ See May 13, 2020 Notice of Data Breach, attached as **Exhibit A**.

26 ⁷ A copy of this May 21, 2020 email is attached as **Exhibit B**.

27 ⁸ A copy of this May 28, 2020 email is attached as **Exhibit C**.

28 ⁹ A copy of the May 14, 2021 press release is attached as **Exhibit D**.

1 SIS but stored on local servers (i.e., the school districts' servers) was also subject to
2 unauthorized access and part of the Data Breach.¹⁰ Aeries' failure to discover this is
3 particularly disturbing as the January 2020 incident referenced in the Notice of Data
4 Breach involved a school district that did not use Aeries Hosting.

5 11. Shockingly, as of the date of filing, Aeries *still* has not publicly disclosed
6 that its non-Aeries Hosting customers may also have had students', parents', and
7 guardians' PII compromised in the Data Breach.

8 12. Aeries is responsible for allowing the Data Breach to occur because it
9 failed to implement and maintain any reasonable safeguards and failed to comply with
10 industry-standard data security practices, contrary to the representations made in
11 Aerie's privacy statements and its explicit and implied agreements with its school
12 district customers.

13 13. During the duration of the Data Breach, Aeries failed to detect the
14 unauthorized third parties' access to its service, notice the massive amounts of data
15 that were compromised, and failed to take any steps to investigate the red flags that
16 should have warned Aeries that its systems were not secure. As a result of Aeries'
17 failure to protect the student information it was entrusted with, Plaintiffs and class
18 members have been exposed to and/or are at a significant risk of identity theft,
19 financial fraud, and other identity-related fraud into the indefinite future. Plaintiffs and
20 class members have also lost the inherent value of their PII. This harm was
21 compounded by Aeries' failure to timely notify its school district customers of the Data
22 Breach, its failure to disclose the extent of the information compromised in the Data
23 Breach, and its further failure to ensure parents and guardians and students of its
24 school district customers received proper and timely notification of the Data Breach.

25
26 ¹⁰ See, e.g., *Aeries Security Incident*, Rocklin Unified School District (May 12, 2020),
27 available at [https://www.rocklinusd.org/documents/District%20Info/RUSD%20-](https://www.rocklinusd.org/documents/District%20Info/RUSD%20-%20Aeries%20Breach%20Parent%20Notification.pdf)
28 [%20Aeries%20Breach%20Parent%20Notification.pdf](https://www.rocklinusd.org/documents/District%20Info/RUSD%20-%20Aeries%20Breach%20Parent%20Notification.pdf).

PARTIES

14. Individual Plaintiffs D.G. and V.G. are the minor children of Individual Plaintiff Anurag Gupta. They are citizens and residents of the State of California and attend public school in ABC, including at the time of the incidents described herein. They entrusted PII to Aeries with the reasonable expectation and understanding that Aeries would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users, and would be timely notified of any data security incidents involving their PII should such occur.

15. Individual Plaintiff Anurag Gupta is a citizen and resident of the State of California. He entrusted PII to Aeries with the reasonable expectation and understanding that Aeries would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users, and would be timely notified of any data security incidents involving his PII should such occur.

16. Class Plaintiff Melinda Tomes is a citizen of the State of Arizona. When she was a California citizen, her children were students in the San Dieguito Union High School District and have since graduated. She entrusted her PII to Aeries with the reasonable expectation and understanding that Aeries would protect and safeguard that information from compromise, disclosure, and misuse by unauthorized users, and would be timely notified of any data security incidents involving his PII should such occur.

17. Aeries is a California corporation with its principal place of business in Anaheim, California. Aeries touts that it offers “industry leading student data management system software.”¹¹ Its primary offering, the Aeries SIS, is used by “over 600 public school districts and education agencies.”¹² While most of these customers are located in California, Aeries also has customers elsewhere in the United States,

¹¹ *Id.*

¹² *Id.*

1 including the state of Texas.¹³ School district customers using Aeries SIS may elect to
 2 have Aeries host student data on Aeries' servers, i.e., Aeries Hosting ("Hosted School
 3 District Customers").

4 **JURISDICTION AND VENUE**

5 18. This Court has subject matter jurisdiction pursuant to the Class Action
 6 Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy
 7 exceeds the sum of \$5,000,000 exclusive of interest and costs, there are more than 100
 8 putative class members, and minimal diversity exists because putative class members
 9 are citizens of a different state than Aeries.

10 19. This Court has personal jurisdiction over Aeries because it is authorized
 11 to and regularly conducts business in California and is headquartered in Anaheim,
 12 California.

13 20. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a
 14 substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in
 15 this District.

16 **FACTUAL ALLEGATIONS**

17 **Aeries and Its Privacy and Data Security Representations**

18 21. Aeries has sold its "Software-as-a-Service" offering, the Aeries SIS, to
 19 over 600 public school districts and education agencies.¹⁴ At least 300 of those are
 20 Hosted School District Customers.¹⁵ Aeries' customers "use Aeries daily to manage
 21 student data on over 2.5 million students."¹⁶

22 22. Aeries is compensated handsomely for the services it provides to its
 23 school district customers. For example, when the Mt. Diablo Unified School District

24 ¹³ <https://www.aeries.com/about/leadership-team> (last visited May 26, 2020)

25 ¹⁴ <https://www.aeries.com/about> (last visited May 26, 2020)

26 ¹⁵ <https://www.aeries.com/about/leadership-team> (last visited May 26, 2020)

27 ¹⁶ <https://www.aeries.com/products/capabilities-advantages> (last visited May 26,
 28 2020)

1 considered purchasing the Aeries SIS offering, it anticipated paying Aeries \$750,000
 2 for the first five years of use, with \$568,350 paid for the first year and costs after the
 3 first year estimated at approximately \$45,000 per year.¹⁷

4 23. Mt. Diablo is but one of at least 600 school district customers of Aeries.
 5 Accordingly, Aeries earns over \$25,000,000 per year in annual revenue from annual
 6 costs alone. The amount is likely significantly greater given the exorbitant first-year
 7 fees Aeries collects when obtaining a new school district customer.

8 24. Aeries is fully aware of the sensitive nature of students' PII stored on or
 9 processed through its systems. It identifies the following categories of "Student Data"
 10 that are managed in its systems: "Medical"; "Discipline"; "Siblings"; "Emergency
 11 Contacts"; "Fees/Fines"; "Counseling"; "Special Ed. / CASEMIS"; "Intervention
 12 Tracking (RTT)"; "Retention Tracking"; "Lockers"; "Photos / ID Cards"; "Custom
 13 Supplemental Data"; "Language Assessment"; "Free & Reduced Lunch"; "Physical
 14 Fitness"; and "Work Permits." The "Medical" category includes items of information
 15 such as "Medical History"; "Immunizations"; "Vaccination Requirements";
 16 "Hearing"; "Vision"; "Physicals"; "Scoliosis"; "Dental"; and "Government Billing."
 17 Other categories of data relevant to students' PII include "Grade Reporting /
 18 Transcripts" and "Testing / Assessment."¹⁸

19 25. An individual student's login credentials, and/or those of their parent or
 20 guardian, may be used to access the PII stored or processed through Aeries' systems
 21 and databases specific to that student/guardian. Other accounts, such as school or
 22

23
 24
 25 ¹⁷ *Agenda Docket Form*, Mt. Diablo Unified School District (January 23, 2007), *available*
 26 *at* <http://esbpublic.mdusd.k12.ca.us/attachments/f8636ff8-fdcb-4b6e-af7c-c1c5b8ba2ed5.pdf>.

27 ¹⁸ <https://www.aeries.com/products/capabilities-advantages> (last visited May 26,
 28 2020)

1 district-level administrators, have access to all or portions of the PII of students and/or
2 guardians within a particular school or district.¹⁹

3 26. When marketing Aeries Hosting, Aeries touts that it “hosts the District
4 Aeries database in a secure off-site data center” and that Aeries Hosting offers
5 “[a]dvanced security encryption.”²⁰

6 27. Beyond specific representations to its Hosted School District Customers,
7 Aeries makes representations to all of its customers and their students’ and those
8 students’ guardians regarding its data security practices. In Aeries’ “Privacy Center” on
9 its website, Aeries states that “it is of paramount priority that Aeries Software designs
10 its products with privacy and security in mind at all time.” The Privacy Center page
11 further represents that Aeries “use[s] the industry best practices to protect data.”²¹

12 28. Aeries’ Privacy Policy, last updated April 24, 2019, makes further
13 representations regarding its data security practices. The Privacy Policy informs users
14 of Aeries’ systems that the PII stored on its systems may include “the following
15 information about students and their guardians: Demographic information such as
16 name, mailing address, email address, and date of birth; Student education records
17 including, but not limited to student’s grades, class enrollment, and behavioral records;
18 Financial information, including but not limited to fees and fines, such as Chromebook
19 insurance, or administrative fees, determined by LEAs; Health-related information
20 including your student’s immunizations and vision and hearing screening results; [and]
21 System usernames and passwords.”²²

22 29. Recognizing the sensitivity of the PII stored on its servers or otherwise
23 processed or managed through Aeries SIS, Aeries’ Privacy Policy further touts that

24 ¹⁹ [https://support.aeries.com/support/solutions/articles/14000067946-aeries-](https://support.aeries.com/support/solutions/articles/14000067946-aeries-security-groups)
25 [security-groups](https://support.aeries.com/support/solutions/articles/14000067946-aeries-security-groups) (last visited May 26, 2020)

26 ²⁰ <https://www.aeries.com/products/aerieshosting> (last visited May 26, 2020)

27 ²¹ <https://www.aeries.com/privacy-center> (last visited May 26, 2020)

28 ²² <https://www.aeries.com/privacy-policy> (last visited August 11, 2020)

1 “Aeries takes various security measures—physical, electronic, and procedural—to help
 2 defend against the unauthorized access and disclosure of your information. . . . [O]ur
 3 employees are required to comply with information security safeguards, and our
 4 systems are protected by technological measures to help prevent unauthorized
 5 individuals from gaining access. Aeries employees are trained to observe and comply
 6 with applicable federal and state privacy laws in the handling, processing, and storage
 7 of your information.”²³

8 30. Aeries’ Privacy Policy also sets forth expectations for Aeries’ behavior in
 9 the event of a data breach, providing that “[u]pon discovery or notification of any
 10 unauthorized access disclosure, Aeries will take immediate measures to safeguard and
 11 prevent further dissemination of any personal information. When reasonably able to
 12 do so, Aeries will notify the impacted parties via contact information on record.”
 13 Aeries represents that it will notify affected users of its system (i.e., students, parents,
 14 and guardians) “via email” and, potentially in addition to email, “in writing” depending
 15 on applicable legal requirements.²⁴

16 **Aeries’ Knowledge That It Was and Is a Target of Cyber Threats**

17 31. Aeries knew it was a prime target for hackers given the significant amount
 18 of sensitive student PII processed through Aeries SIS and stored in Aeries Hosting.
 19 Indeed, on the Privacy Center webpage, when touting its data security practices, Aeries
 20 acknowledges the “risks involved by schools utilizing its products and services for
 21 student data collection and retention.”²⁵

22 32. Aeries’ knowledge is underscored by massive data breaches of other
 23 companies offering educational software products and services. For example, in July
 24 2019, the educational software company Pearson announced a data breach that
 25

26 ²³ *Id.*

27 ²⁴ *Id.*

28 ²⁵ <https://www.aeries.com/privacy-center> (last visited May 26, 2020)

1 affected approximately “13,000 of the company’s school and university accounts”; in
 2 one state alone, Nevada, the Pearson data breach resulted in “[m]ore than 650,000
 3 Nevada students ha[ving] personal information exposed.”²⁶

4 33. The Pearson data breach was not an isolated incident. According to The
 5 K-12 Cybersecurity Resource Center, in 2019 alone K-12 public school districts and
 6 education agencies across the U.S. suffered a total of 348 publicly acknowledged data
 7 security incidents – “a rate of nearly two incidents per school day over the course of
 8 2019.”²⁷ Approximately 60% of these data security incidents were “data breaches,
 9 primarily involving the unauthorized disclosure of student data.”²⁸

10 34. Despite being a holder of PII for tens, if not hundreds of thousands of
 11 minor students, Aeries failed to prioritize data security by adopting reasonable data
 12 security measures to prevent and detect unauthorized access to their highly sensitive
 13 systems and databases. Aeries had the resources to prevent a breach, but neglected to
 14 adequately invest in data security, despite the growing number of well-publicized data
 15 breaches affecting educational institutions and their vendors.

16 35. Despite these well-publicized breaches of educational institutions and
 17 educational vendors, Aeries failed to undertake adequate analyses and testing of its
 18 own systems, training of its own personnel, and other data security measures to ensure
 19 that similar vulnerabilities were avoided or remedied and that Plaintiffs’ and class
 20 members’ PII was protected.

22
 23 ²⁶ Amanda Pak-Harvey, *Nevada students’ information exposed in data breach*, Las Vegas
 24 Review-Journal (Aug. 2, 2019),
 25 <https://www.reviewjournal.com/local/education/nevada-students-information-exposed-in-data-breach-1817032/>

26 ²⁷ *K-12 Cybersecurity 2019 Year in Review: Part III: Cybersecurity Incidents: 2019*, The K-12
 27 Cybersecurity Resource Center, <https://k12cybersecure.com/year-in-review/2019-incidents/> (last visited May 26, 2020).

28 ²⁸ *Id.*

The Data Breach

36. In November 2019, Aeries learned that unauthorized persons had attempted to access data through Aeries SIS and conducted an internal investigation. Aeries contends that no actual unauthorized access was uncovered during this investigation.

37. Nonetheless, on December 20, 2019, Aeries updated the Aeries SIS offering to fix known security deficiencies following its internal investigation.

38. In January 2020, Aeries learned that one of its school district clients whose students' (as well as the students' parents' and guardians') personal information was stored locally on the school district's database and processed through the Aeries SIS, had its local database subjected to unauthorized access. Aeries undertook another investigation in cooperation with the school district customer, local law enforcement, and federal authorities.

39. Aeries contends that it was not until March 2020 that it discovered the unauthorized access of other databases in Aeries Hosting.

40. Specifically, at least 166 databases in Aeries Hosting were subject to unauthorized access beginning on or about November 4, 2019. According to Aeries, "the unauthorized access has been terminated." However, Aeries has not disclosed when such access was terminated or what, if anything, was done to avoid future security incidents.

41. Class Plaintiff alleges that the San Dieguito Union High School District was specifically targeted in the breach, and the residents of that district are at greater risk than the residents of other school districts.

42. Despite having knowledge of the Data Breach as early as November 2019, and certainly no later than January 2020, Aeries did not notify its school district customers of the Data Breach until April 27, 2020, when it issued a "Notice of Data Breach."

1 43. The April 27, 2020 “Notice of Data Breach” disclosed only that the
2 following personal information was compromised: “Parent and Student Login
3 information, physical residence addresses, emails, and ‘password hashes.’” Aeries
4 further acknowledged that “[w]ith access to a password hash, weak, common or simple
5 passwords, can be deconstructed to gain unauthorized access to Parent and Student
6 Accounts.”

7 44. The Notice of Data Breach did not disclose that additional treasure
8 troves of PII were stored on behalf of its school district customers, including, inter
9 alia, minor students’ immunization and other health records, social security numbers,
10 class grades, standardized test information, previous addresses, as well as the
11 information on students, parents, and guardians identified in paragraphs 22 and 26 of
12 this Complaint.

13 45. More than two weeks after Aeries sent its school district customers the
14 Notice of Data Breach, SDUHSD on May 14, 2020 finally issued a press release
15 (**Exhibit D**) stating:

16 While SDUHSD was unable to confirm whether any
17 information was accessed or acquired by the unauthorized
18 individual, the investigation confirmed that the following
19 types of information were present in the affected email
20 accounts: name, address, Social Security number, driver's
21 license/state identification number, passport number,
22 financial account number, diagnosis information, medical
information, health insurance information, and
username/password/account login.

23 46. The above information had previously been collected by the school
24 districts and, upon information and belief, was also stored in Aeries.

25 47. However, SDUHSD dubiously asserts “Although it has no confirmation
26 that personal information was acquired without authorization” But Plaintiffs have
27 every reason to believe this information was in fact compromised because SDUHSD
28

1 stated that “While the investigation was unable to determine the scope of information
2 that was actually accessed within the affected email accounts, SDUHSD is notifying
3 potentially affected individuals in an abundance of caution.”

4 48. Plaintiffs’ reasonable belief that this information was compromised is
5 underscored by the wholly inadequate investigation Aeries has undertaken to date,
6 which failed to identify the Data Breach for several months after the first unauthorized
7 access attempts were identified.

8 49. Because of the nature of the PII stored or processed by Aeries, and the
9 nature of the hack targeting both locally hosted and Aeries-hosted customers, Plaintiffs
10 understand that all categories of PII were subject to unauthorized access and
11 exfiltration, theft, or disclosure. In other words, criminals would have no purpose for
12 hacking Aeries other than to exfiltrate or steal the coveted PII stored or processed by
13 Aeries.

14 50. Unfortunately, even Aeries’ subsequent investigations were inadequate.
15 They failed to uncover that it was not only the student, parent, and guardian PII stored
16 on Aeries Hosting that was compromised. In early May 2020, other school district
17 customers discovered that students’, parents’, and guardians’ PII processed through
18 the Aeries SIS but stored on local servers (i.e., the school districts’ servers) was also
19 subject to unauthorized access.

20 51. As of the date of filing, Aeries still has not publicly disclosed that its non-
21 Aeries Hosting customers using local servers had students’, parents’, and guardians’
22 PII compromised in the Data Breach.

23 52. None of the communications from Aeries, nor the communications the
24 Plaintiffs received from the school districts, offered victims of the Data Breach any
25 type of identity or fraud monitoring or identity theft protection services. Notably, other
26
27
28

1 companies have provided automatic identity-theft protection services to victims of
2 similar breaches, including in relation to the aforementioned Pearson data breach.²⁹

3 53. Aeries' response to the Data Breach caused confusion among the victims
4 of the data breach, resulting in class members spending time, and continuing to spend
5 a significant amount of time into the future, taking measures to protect themselves
6 from identity theft, fraud, and other identity-related crimes.

7 54. Aeries is responsible for allowing the Data Breach to occur because it
8 failed to implement and maintain any reasonable safeguards and failed to comply with
9 industry-standard data security practices, contrary to the representations made in
10 Aeries' privacy statements and its explicit and implied agreements with its users.

11 55. During the duration of the Data Breach, Aeries failed to detect the
12 unauthorized third parties' access to its systems and databases, notice the massive
13 amounts of data that were compromised, and failed to take any steps to investigate the
14 red flags that should have warned Aeries that its systems were not secure. As a result
15 of Aeries' failure to protect the sensitive PII it was entrusted with, Class Plaintiffs and
16 class members are at a significant risk of identity theft, financial fraud, and other
17 identity-related fraud into the indefinite future. Class Plaintiffs and class members have
18 also lost the inherent value of their PII.

19 56. Plaintiffs and class members provided their PII to Aeries and its school
20 district customers with the expectation and understanding that Aeries would
21 adequately protect and store their data. If Plaintiffs and class members had known that
22 Aeries data security was insufficient to protect their PII, they would have demanded
23 that their school districts not store their PII on Aeries' databases or process it through
24 Aeries' systems.

25
26 ²⁹ See, e.g., *Students and Schools Affected by Pearson Data Breach*, Identity Theft Resource
27 Center, [https://www.idtheftcenter.org/students-and-schools-affected-by-pearson-](https://www.idtheftcenter.org/students-and-schools-affected-by-pearson-data-breach/)
28 [data-breach/](https://www.idtheftcenter.org/students-and-schools-affected-by-pearson-data-breach/) (last visited May 26, 2020).

**Aeries Failed to Comply with Regulatory Guidance and Meet Consumers’
Expectations**

57. Federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the FTC has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.³⁰

58. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.³¹ Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.³²

59. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested

³⁰ Federal Trade Commission, *Start With Security* (June 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited May 26, 2020).

³¹ Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

³² *Id.*

1 methods for security; monitor for suspicious activity on the network; and verify that
2 third-party service providers have implemented reasonable security measures.³³

3 60. The FTC has brought enforcement actions against businesses for failing
4 to adequately and reasonably protect customer information, treating the failure to
5 employ reasonable and appropriate measures to protect against unauthorized access to
6 confidential consumer data as an unfair act or practice prohibited by Section 5 of the
7 Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions
8 further clarify the measures businesses must take to meet their data security
9 obligations.³⁴

10 61. In this case, Aeries was fully aware of its obligation to use reasonable
11 measures to protect the PII of its customers, acknowledging as much in its own privacy
12 policies. Aeries also knew it was a target for hackers. But despite understanding the
13 consequences of inadequate data security, Aeries failed to comply with industry-
14 standard data security requirements.

15 62. Aeries' failure to employ reasonable and appropriate measures to protect
16 against unauthorized access to students', parents', and guardians' PII constitutes an
17 unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 and
18 various state consumer protection and data breach statutes.

19 **Effect of the Data Breach**

20 63. Aeries' failure to keep Plaintiffs' and class members' PII secure has severe
21 ramifications. Given the sensitive nature of the PII stolen in the Data Breach, cyber
22 criminals have the ability to commit identity theft and other identity-related fraud
23 against Plaintiffs and class members now and into the indefinite future.

24
25 ³³ FTC, *Start With Security*, *supra* note 27.

26 ³⁴ Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*,
27 <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> (last visited May 26, 2020).
28

64. The information stolen from Aeries included usernames and passwords—PII that is highly valued among cyber thieves and criminals on the Dark Web. For example, Apple ID usernames and passwords were sold on average for \$15.39 each on the Dark Web, making them the most valuable non-financial credentials for sale on that marketplace. Usernames and passwords for eBay (\$12), Amazon (\leq \$10), and Walmart (\leq \$10) fetch similar amounts.³⁵ Consumers often reuse passwords. By unlawfully obtaining this information, cyber criminals can use these credentials to access other services beyond that which was hacked.

65. Other information stored on Aeries' databases that were compromised in the Data Breach can fetch far more on the Dark Web. For example, detailed student health records were stored on the compromised databases. Stolen medical records “can fetch up to \$350 on the dark web.”³⁶

66. PII also has significant monetary value in part because criminals continue their efforts to obtain this data.³⁷ In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. Instead, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,473 data

³⁵ Don Reisinger, *Here's How Much Your Stolen Apple ID Login Costs on the Dark Web*, Fortune (March 7, 2018), <https://fortune.com/2018/03/07/apple-id-dark-web-cost/>. See also <https://www.npr.org/2018/02/22/588069886/take-a-peek-inside-the-market-for-stolen-usernames-and-passwords> (last visited May 26, 2020).

³⁶ *How Cybercriminals Make Money: How much is your information worth to a cybercriminal via the Dark Web?*, Keeper Security, <https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html> (last visited May 26, 2020).

³⁷ *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, CIO Magazine (Sept. 28, 2014), available at <http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html>.

1 breaches in 2019, which represents a 17 percent increase from the total number of
2 breaches reported in 2018.³⁸

3 67. The value of PII is key to unlocking many parts of the financial sector
4 for consumers. Whether someone can obtain a mortgage, credit card, business loan,
5 tax return, or even apply for a job depends on the integrity of their PII. Similarly, the
6 businesses that request (or require) consumers to share their PII as part of a
7 commercial transaction do so with the expectation that its integrity has not been
8 compromised.

9 68. Aeries recognizes the value of PII, as its possession and processing of
10 PII allows it to advance its own commercial or economic interests. Aeries shares the
11 PII stored or processed through Aeries' systems and servers with other entities in order
12 to create new software applications, or integrations with other companies' existing
13 software applications, that it can then sell for an increased profit to its school district
14 customers.³⁹

15 69. Annual monetary losses for victims of identity theft are in the billions of
16 dollars. In 2017, fraudsters stole \$16.8 billion from consumers in the United States,
17 which includes \$5.1 billion stolen through bank account take-overs.⁴⁰

21 ³⁸ 2019 End-of-Year Data Breach Report (2019), Identity Theft Resource Center, *available*
22 *at* [https://www.idtheftcenter.org/wp-](https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf)
23 [content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-](https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf)
24 [Report_FINAL_Highres-Appendix.pdf](https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf).

25 ³⁹ *See, e.g.*, News & Press Releases, Aeries, *available at*
26 <https://www.aeries.com/about/news-and-press-releases> (last visited August 11,
27 2020) (describing new offerings available for purchase arising from integration of
28 Aeries' software with offerings of other companies).

⁴⁰ Javelin, *2018 Identity fraud: Fraud Enters A New Era of Complexity*, *available at*
[https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-](https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity)
[new-era-complexity](https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity) (last visited May 26, 2020).

1 70. The annual cost of identity theft is even higher. McAfee and the Center
2 for Strategic and International Studies estimates that the likely annual cost to the global
3 economy from cybercrime is \$445 billion a year.⁴¹

4 71. The foregoing problems are compounded where, as with Individual
5 Plaintiffs D.G. and V.G., the victims of the Data Breach are minors.

6 72. Over 1 million minor children were victims of fraud or identity theft in
7 2017, and two-thirds of those victims were under the age of seven.⁴²

8 73. Data thieves are also more likely to target minors' PII and to use that PII
9 once it is stolen. In 2017, "[a]mong notified breach victims . . . 39 percent of minors
10 became victims of fraud, versus 19 percent of adults."⁴³

11 74. Criminals make use of minors' PII to open accounts or new lines of credit
12 that may not be noticed by the minor; and to create "synthetic identities" using a
13 combination of real and fictitious information which again, the minor may not realize
14 was stolen.⁴⁴ Because minors do not regularly monitor their bank accounts (if they have
15 them) or their credit reports, data thieves are more likely to make unrestricted use of
16 this information for longer periods of time than they would for adult victims.⁴⁵

17 75. Minors also generally are less likely to receive notice from the company
18 responsible for the data breach or to even realize that a thief has made fraudulent use
19 of their information in other ways – such as creating a new identity for the purposes
20

21 ⁴¹ Insurance Information Institute, *Facts + Statistics: Identity theft and cybercrime*, available
22 at <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (last
visited May 26, 2020).

23 ⁴² Kelli B. Grant, *Identity Theft isn't just an adult problem. Kids are victims, too*, CNBC
24 (April 24, 2018), <https://www.cnbc.com/2018/04/24/child-identity-theft-is-a-growing-and-expensive-problem.html>.

25 ⁴³ *Id.*

26 ⁴⁴ *Id.*

27 ⁴⁵ Ron Lieber, *Identity Theft Poses Extra Troubles for Children*, N.Y. Times (April 16,
28 2015), <https://www.nytimes.com/2015/04/18/your-money/a-childs-vulnerability-to-identity-theft.html>.

1 of accessing government benefits, healthcare, or employment.⁴⁶ Minors often “won’t
 2 find out that their identity has been stolen until they apply for their first credit card or
 3 college loan.”⁴⁷

4 76. Children are also particularly susceptible to physical harm in the event of
 5 a data breach. Data thieves can use their PII “to link a child to his or her parents and
 6 pinpoint the child’s physical address.”⁴⁸ This risk is particularly disturbing in light of
 7 the student PII stored or processed by Aeries, which in some instances includes teacher
 8 and home room information – allowing criminals to target children with even greater
 9 precision.

10 77. Reimbursing a consumer for a financial loss due to fraud does not make
 11 that individual whole again. On the contrary, in addition to the irreparable damage that
 12 may result from the theft of PII, identity theft victims must spend numerous hours
 13 and their own money repairing the impact to their credit. After conducting a study, the
 14 Department of Justice’s Bureau of Justice Statistics found that identity theft victims
 15 “reported spending an average of about 7 hours clearing up the issues” and resolving
 16 the consequences of fraud in 2014.⁴⁹

17 78. Even before the occurrence of identity theft, victims may spend valuable
 18 time and suffer from the emotional toll of a data breach. Shortly after learning of the
 19 breach, Individual Plaintiff Gupta spent approximately two hours investigating the
 20

21 ⁴⁶ *Id.*

22 ⁴⁷ Larry Magid, *Teens Vulnerable to Identity Theft, Financial Crimes, and Impersonation*,
 23 Forbes (Nov. 7, 2013),
<https://www.forbes.com/sites/larrymagid/2013/11/07/teens-concerned-about-identity-theft/#6ab243211c49>.

24 ⁴⁸ Daniel Victor, *Security Breach at Toy Maker Vtech Includes Data on Children*, N.Y.
 25 Times (Nov. 30, 2015), <https://www.nytimes.com/2015/12/01/business/security-breach-at-toy-maker-vtech-includes-data-on-children.html>.

26 ⁴⁹ U.S. Department of Justice, *Victims of Identity Theft, 2014* (Revised November 13,
 27 2017), available at <http://www.bjs.gov/content/pub/pdf/vit14.pdf> (last visited May
 28 26, 2020).

1 Data Breach after receiving notice from ABC, including independent online research
 2 regarding the scope of the breach and communicating with ABC regarding the breach.
 3 The Plaintiffs expend time monitoring their credit and other identity-related
 4 information and explored options for identity theft protection services because Aeries
 5 did not offer such services as a result of the Data Breach.

6 79. The impact of identity theft can have ripple effects, which can adversely
 7 affect the future financial trajectories of victims' lives. For example, the Identity Theft
 8 Resource Center reports that respondents to their surveys in 2013-2016 described that
 9 the identity theft they experienced affected their ability to get credit cards and obtain
 10 loans, such as student loans or mortgages.⁵⁰ For some victims, this could mean the
 11 difference between going to college or not, becoming a homeowner or not, or having
 12 to take out a high interest payday loan versus a lower-interest loan.

13 80. It is no wonder, then, that identity theft exacts a severe emotional toll on
 14 its victims. The 2017 Identity Theft Resource Center survey⁵¹ evidences the emotional
 15 suffering experienced by victims of identity theft:

- 16 • 75% of respondents reported feeling severely distressed;
- 17 • 67% reported anxiety;
- 18 • 66% reported feelings of fear related to personal financial safety;
- 19 • 37% reported fearing for the financial safety of family members;
- 20 • 24% reported fear for their physical safety;
- 21 • 15.2% reported a relationship ended or was severely and negatively
- 22 impacted by the identity theft; and
- 23 • 7% reported feeling suicidal.

24
 25 ⁵⁰ Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, available at
 26 https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited
 27 May 26, 2020).

28 ⁵¹ *Id.*

1 81. Identity theft can also exact a physical toll on its victims. The same survey
2 reported that respondents experienced physical symptoms stemming from their
3 experience with identity theft:

- 4 • 48.3% of respondents reported sleep disturbances;
- 5 • 37.1% reported an inability to concentrate / lack of focus;
- 6 • 28.7% reported they were unable to go to work because of physical
7 symptoms;
- 8 • 23.1% reported new physical illnesses (aches and pains, heart
9 palpitations, sweating, stomach issues); and
- 10 • 12.6% reported a start or relapse into unhealthy or addictive
11 behaviors.⁵²

12 82. There may also be a significant time lag between when PII is stolen and
13 when it is actually misused. According to the U.S. Government Accountability Office,
14 which conducted a study regarding data breaches:

15 [L]aw enforcement officials told us that in some cases,
16 stolen data may be held for up to a year or more before
17 being used to commit identity theft. Further, once stolen
18 data have been sold or posted on the Web, fraudulent use
19 of that information may continue for years. As a result,
20 studies that attempt to measure the harm resulting from
data breaches cannot necessarily rule out all future harm.⁵³

21 83. The risk of identity theft is particularly acute where detailed personal
22 information is stolen, such as the PII that was compromised in the Data Breach.

26 ⁵² *Id.*

27 ⁵³ U.S. Government Accountability Office, *Report to Congressional Requesters* (June
28 2007), <http://www.gao.gov/new.items/d07737.pdf>.

1 84. As the result of the Data Breach, Plaintiffs and class members have
2 suffered or will suffer economic loss and other actual harm for which they are entitled
3 to damages, including, but not limited to, the following:

- 4 a. identity theft and fraud resulting from theft of their PII;
- 5 b. costs associated with the detection and prevention of identity theft and
6 unauthorized use of their online accounts, including financial accounts;
- 7 c. losing the inherent value of their PII;
- 8 d. losing the value of Aeries' explicit and implicit promises of adequate data
9 security;
- 10 e. costs associated with purchasing credit monitoring and identity theft
11 protection services;
- 12 f. unauthorized access to and misuse of their online accounts;
- 13 g. unauthorized charges and loss of use of and access to their financial account
14 funds and costs associated with inability to obtain money from their
15 accounts or being limited in the amount of money they were permitted to
16 obtain from their accounts, including missed payments on bills and loans,
17 late charges and fees, and adverse effects on their credit;
- 18 h. lowered credit scores resulting from credit inquiries following fraudulent
19 activities;
- 20 i. costs associated with time spent and the loss of productivity or enjoyment
21 of one's life from taking time to address and attempt to mitigate and address
22 the actual and future consequences of the Data Breach, including
23 discovering fraudulent charges, cancelling and reissuing cards, addressing
24 other varied instances of identity theft – such as credit cards, bank accounts,
25 loans, government benefits, and other services procured using the stolen PII,
26 purchasing credit monitoring and identity theft protection services, imposing
27 withdrawal and purchase limits on compromised accounts, updating login
28

1 information for online accounts sharing the same login credentials as were
2 compromised in the Data Breach, and the stress, nuisance, and annoyance
3 of dealing with the repercussions of the Data Breach;

4 j. the continued imminent and certainly impending injury flowing from
5 potential fraud and identity theft posed by their PII being in the possession
6 of one or more unauthorized third parties; and

7 k. continued risk of exposure to hackers and thieves of their PII, which remains
8 in Aeries' possession and is subject to further breaches so long as Aeries fails
9 to undertake appropriate and adequate measures to protect Plaintiffs and
10 class members.

11 85. Additionally, Plaintiffs and class members place significant value in data
12 security. According to a recent survey conducted by cyber-security company FireEye,
13 approximately 50% of consumers consider data security to be a main or important
14 consideration when making purchasing decisions and nearly the same percentage
15 would be willing to pay more in order to work with a provider that has better data
16 security. Likewise, 70% of consumers would provide less personal information to
17 organizations that suffered a data breach.⁵⁴

18 86. The cost of hosting or processing students', parents', and guardians PII
19 on or through Aeries' databases and systems includes things such as the actual cost of
20 the servers and employee hours needed to process said transactions. One component
21 of the cost of using these services is the explicit and implicit promises Aeries made to
22 protect students', parents', and guardians' PII. Because of the value students and their
23 parents and guardians place on data privacy and security, companies with robust data
24 security practices can command higher prices than those who do not. Indeed, if
25

26 ⁵⁴ FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016),
27 [https://www.fireeye.com/blog/executive-](https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html)
28 [perspective/2016/05/beyond_the_bottomli.html](https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html).

1 students, parents, guardians, and school districts did not value their data security and
 2 privacy, companies like Aeries would have no reason to tout their data security efforts
 3 to their actual and potential customers.

4 87. Had the victims of the Data Breach including Plaintiffs known the truth
 5 about Aeries' data security practices—that Aeries would not adequately protect and
 6 store their data—they would have demanded that their school districts not store their
 7 PII on Aeries' databases or process it through Aeries' systems.

8 88. Class Plaintiffs and class members are at an imminent risk of fraud,
 9 criminal misuse of their PII, and identity theft for years to come as result of the data
 10 breach and Aeries' deceptive and unconscionable conduct.

11 **CLASS ACTION ALLEGATIONS**

12 89. Pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2) and (b)(3),
 13 Class Plaintiff seeks certification of the following class:

14 All individuals in the United States who had an Aeries
 15 account through the San Dieguito Union High School
 16 District at the time of the Data Breach.

17 90. Excluded from the Class are any school districts or educational agencies
 18 that are Aeries customers, Aeries itself, any entity in which Aeries has a controlling
 19 interest, and Aeries' officers, directors, legal representatives, successors, subsidiaries,
 20 and assigns. Also excluded from the Class are any judicial officer presiding over this
 21 matter, members of their immediate family, members of their judicial staff, and any
 22 judge sitting in the presiding court system who may hear an appeal of any judgment
 23 entered.

24 91. **Risk of Inconsistent or Varying Adjudications. Fed. R. Civ. P.**
 25 **23(b)(1).** As the proposed class members include tens, if not hundreds, of thousands
 26 of students and their parents or guardians, there is significant risk of inconsistent or
 27 varying adjudications with respect to individual class members that would establish
 28

1 incompatible standards of conduct for Aeries. For example, injunctive relief may be
2 entered in multiple cases, but the ordered relief may vary, causing Aeries to have to
3 choose between differing means of upgrading its data security infrastructure and
4 choosing the court order with which it will comply. Class action status is also
5 warranted because prosecution of separate actions by the members of the Class
6 would create a risk of adjudications with respect to individual members of the Class
7 that, as a practical matter, would be dispositive of the interests of other members not
8 parties to this action, or that would substantially impair or impede their ability to
9 protect their interests.

10 92. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1),
11 the members of the Class are so numerous and geographically dispersed that the
12 joinder of all members is impractical. While the exact number of class members is
13 unknown to Class Plaintiff at this time, it is estimated to have approximately 100,000
14 members.

15 93. **Commonality and Predominance. Fed. R. Civ. P. 23(a)(2) and**
16 **(b)(3).** This action involves common questions of law and fact that predominate over
17 any questions affecting individual class members. The common questions include, but
18 are not limited to:

19 a. Whether Aeries knew or should have known that its computer and data
20 storage systems were vulnerable to attack;

21 b. Whether Aeries omitted or misrepresented material facts regarding the
22 security of its computer and data storage systems and their inability to protect vast
23 amounts of sensitive data, including Class Plaintiff's and class members' PII;

24 c. Whether Aeries failed to take adequate and reasonable measures to
25 ensure such computer and data systems were protected;

26 d. Whether Aeries failed to take available steps to prevent and stop the Data
27 Breach from happening;

1 e. Whether Aeries failed to disclose the material facts that it did not have
2 adequate computer systems and security practices to safeguard PII;

3 f. Whether Aeries owed duties to Class Plaintiff and class members to
4 protect their PII;

5 g. Whether Aeries owed a duty to provide timely and accurate notice of the
6 Data Breach to Class Plaintiff and class members;

7 h. Whether Aeries breached its duties to protect the PII of Class Plaintiff
8 and class members by failing to provide adequate data security;

9 i. Whether Aeries breached its duty to provide timely and accurate notice
10 of the Data Breach to Class Plaintiff and class members;

11 j. Whether Aeries' failure to secure Class Plaintiff's and class members' PII
12 in the manner alleged violated federal, state and local laws, or industry standards;

13 k. Whether Aeries was negligent, reckless or intentionally indifferent in its
14 representations to Plaintiffs and class members concerning its security protocols;

15 l. Whether Aeries' conduct and practices described herein amount to acts
16 of intrusion upon seclusion;

17 m. Whether Aeries was negligent in making misrepresentations to Class
18 Plaintiff and class members;

19 n. Whether Aeries was negligent in establishing, implementing, and
20 following security protocols;

21 o. Whether the Class Plaintiff's and class members' PII was compromised
22 and exposed as a result of the Data Breach and the extent of that compromise and
23 exposure;

24 p. Whether Aeries' conduct, including its failure to act, resulted in or was
25 the proximate cause of the Data Breach, resulting in the unauthorized access to and/or
26 theft of Class Plaintiff's and class members' PII;

1 q. Whether Aeries has a contractual obligation to use reasonable security
2 measures and whether it complied with such contractual obligation;

3 r. Whether Class Plaintiff and class members were the intended third-party
4 beneficiaries of any contractual obligations owed by Aeries;

5 s. Whether Aeries' conduct amounted to violations of California consumer
6 protection and data breach statutes;

7 t. Whether, as a result of Aeries' conduct, Class Plaintiff and class members
8 face a significant threat of harm and/or have already suffered harm, and, if so, the
9 appropriate measure of damages to which they are entitled;

10 u. Whether, as a result of Aeries' conduct, Class Plaintiff and class members
11 are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the
12 nature of such relief;

13 v. Whether Class Plaintiff and class members are entitled to compensatory
14 damages;

15 w. Whether the Class Plaintiff and class members are entitled to punitive
16 damages; and

17 x. Whether the Class Plaintiff and class members are entitled to statutory
18 damages.

19 94. **Typicality. Fed. R. Civ. P. 23(a)(3).** Class Plaintiff's claims are typical
20 of other class members' claims because Class Plaintiff and class members were
21 subjected to the same allegedly unlawful conduct and damaged in the same way.

22 95. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4),
23 Class Plaintiff is an adequate representative of the Class. Class Plaintiff is a member of
24 the Class. Class Plaintiff has no conflict of interest with the Class. Plaintiffs' counsel
25 are competent and experienced in litigating class actions, including extensive
26 experience in data breach and privacy litigation and consumer protection claims. Class
27
28

96. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs and class members may not be sufficient to justify individual litigation. Here, the damages suffered by Class Plaintiff and the class members are relatively small compared to the burden and expense required to individually litigate their claims against Aeries, and thus, individual litigation to redress Aeries' wrongful conduct would be impracticable. Individual litigation by each class member would also strain the court system. Moreover, individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

8 97. **Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2).** Class
9 certification is also appropriate under Rule 23(b)(2). Aeries, through its uniform
10 conduct, acted or refused to act on grounds generally applicable to the Class as a whole,
11 making injunctive and declaratory relief appropriate to the Class as a whole. Moreover,
12 Aeries continues to maintain its inadequate security practices, retains possession of
13 Class Plaintiff's and the class members' PII, and has not been forced to change its
14 practices or to relinquish PII by nature of other civil suits or government enforcement
15 actions, thus making injunctive and declaratory relief a live issue and appropriate to
16 the Class as a whole.

* * *

Count 1

NEGLIGENCE

Against Aeries on Behalf of Individual Plaintiffs and Class Plaintiff and the Class

98. Plaintiffs repeat the allegations in paragraphs 1 – 97 in this Complaint, as if fully alleged herein.

99. Aeries, in offering educational software, knew that Plaintiffs and class members' sensitive PII would be stored or processed by Aeries systems and databases, including in Aeries Hosting. Aeries in fact stored (i.e., for school districts using Aeries Hosting) and/or processed (i.e., for school districts using Aeries Hosting and for school districts using local servers) this PII through and on its computer systems and/or databases.

100. The class members that are minors are particularly vulnerable and defenseless group of Aeries users and are more significantly damaged and imminently threatened to be damaged as a result of Aeries' negligence described herein because, without limitation, they are especially: (1) attractive targets to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or identity theft; and (4) subject to prolonged surreptitious fraud and identity theft following the theft of their data, all of which is well documented in academic and government-issued materials, by experts in the field, and by the media.

101. By collecting, storing, and using this data, Aeries had a duty of care to Plaintiffs and class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting this PII in Aeries' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Aeries' security systems and data storage architecture to ensure that Plaintiffs' and class members' PII was adequately secured and protected; (b)

1 implementing processes that would detect an unauthorized breach of Aeries' security
2 systems and data storage architecture in a timely manner; (c) timely acting on all
3 warnings and alerts, including public information, regarding Aeries' security
4 vulnerabilities and potential compromise of the PII of Plaintiffs and class members;
5 (d) maintaining data security measures consistent with industry standards and
6 applicable state and federal law; and (e) timely and adequately informing Plaintiffs and
7 class members if and when a data breach occurred notwithstanding undertaking (a)
8 through (d) above.

9 102. Aeries had common law duties to prevent foreseeable harm to Plaintiffs
10 and class members. These duties existed because Plaintiffs and class members were
11 the foreseeable and probable victims of any inadequate security practices. In fact, not
12 only was it foreseeable that Plaintiffs and class members would be harmed by the
13 failure to protect their PII because hackers routinely attempt to steal such information
14 and use it for nefarious purposes, Aeries knew that it was more likely than not Plaintiffs
15 and other class members would be harmed by such theft.

16 103. Aeries had a duty to monitor, supervise, control, or otherwise provide
17 oversight to safeguard the PII that was collected, stored, and processed by Aeries
18 computer systems.

19 104. Aeries' duties to use reasonable security measures also arose as a result of
20 the special relationship that existed between Aeries, on the one hand, and Plaintiffs
21 and class members, on the other hand. The special relationship arose because Plaintiffs
22 and class members entrusted Aeries with their PII by virtue of their participation in all
23 aspects of school life. Aeries alone could have ensured that its security systems and
24 data storage architecture were sufficient to prevent or minimize the Data Breach.

25 105. Aeries' duties to use reasonable data security measures also arose under
26 Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which
27 prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and
28

1 enforced by the FTC, the unfair practice of failing to use reasonable measures to
2 protect PII. Various FTC publications and data security breach orders further form
3 the basis of Aeries' duties. In addition, individual states have enacted statutes based
4 upon the FTC Act that also created a duty. Plaintiffs and class members are consumers
5 within the class of persons Section 5 of the FTC Act (and similar state statutes) were
6 intended to protect.

7 106. Aeries' duties to use reasonable data security measures also arose under
8 the California Consumer Privacy Act ("CCPA), Cal. Civ. Code § 1798.100, *et seq.*, which
9 imposes a "duty to implement and maintain reasonable security procedures and
10 practices appropriate to the nature of the information to protect the personal
11 information." Other states have statutes that impose a substantially similar duty of
12 care.

13 107. The harm that has occurred is the type of harm the FTC Act (and similar
14 state statutes) and the CCPA (and similar statutes of other states) were intended to
15 guard against. Indeed, the FTC has pursued over fifty enforcement actions against
16 businesses which, as a result of defendants' failure to employ reasonable data security
17 measures and avoid unfair and deceptive practices, caused the same harm suffered by
18 Plaintiffs and class members.

19 108. Aeries owed heightened duties to Plaintiffs D.G. and V.G. and the minor
20 class members, and Aeries was aware of the heightened vulnerability and damage that
21 would be suffered by Plaintiffs D.G. and V.G. and the minor class members in the
22 event of a data breach.

23 109. Aeries knew or should have known that its computer systems and data
24 storage architecture were vulnerable to unauthorized access and targeting by hackers
25 for the purpose of stealing and misusing confidential PII.

26 110. Aeries knew or should have known that a breach of its systems and data
27 storage architecture would inflict millions of dollars of damages upon Plaintiffs and
28

1 the Class, and Aeries was therefore charged with a duty to adequately protect this
2 critically sensitive information.

3 111. Aeries breached the duties it owed to Plaintiffs and class members
4 described above, including the heightened duties owed to Plaintiffs D.G. and V.G. and
5 minor class members, and thus was negligent. Aeries breached these duties by, among
6 other things, failing to: (a) exercise reasonable care and implement adequate security
7 systems, protocols and practices sufficient to protect the PII of Plaintiffs and class
8 members; (b) detect the breach while it was ongoing; (c) maintain security systems
9 consistent with industry standards; (d) and timely and adequately informing its
10 customers of the fact and extent of the Data Breach. These failures constituted both
11 violations of the FTC Act (and similar state statutes), and the CCPA (and similar
12 statutes from other states), as well as a breach of duties owed to Plaintiffs and class
13 members under the common law. Aeries' violation of the FTC Act (and similar state
14 statutes) and the CCPA (and similar statutes from other states) constitutes negligence
15 *per se* and establishes the elements of duty and breach.

16 112. Aeries also failed to exercise reasonable care and breached its common
17 law duties when it falsely conveyed information to its Hosted School District
18 Customers in its April 27, 2020 "Notice of Data Breach," which misrepresentation
19 failed to sufficiently convey the scope of PII potentially compromised the Data Breach;
20 provided the thieves and/or subsequent unauthorized recipients of the stolen
21 information with additional time and cover to further purloin and re-sell the stolen PII
22 belonging to Plaintiffs and the Class; provided the thieves and the purchasers and/or
23 other subsequent unauthorized recipients with an opportunity to directly defraud
24 Plaintiffs and the Class; failed to adequately apprise its school district customers of the
25 need to promptly notify Plaintiffs and the Class of the fact that their PII was
26 compromised and in imminent jeopardy of falling further into the hands of cyber
27 criminals; and failed to directly notify Plaintiffs and the Class of the same.

113. But for Aeries' wrongful and negligent breach of its duties owed to Plaintiffs and class members, their PII would not have been compromised.

114. As a direct and proximate result of Aeries' negligence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach investigating the nature of the Data Breach not fully disclosed by Aeries, reviewing bank statements, payment card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Count 2

DECLARATORY JUDGMENT

Against Aeries on Behalf of Individual Plaintiffs and Class Plaintiff and the Class

115. Plaintiffs repeat the allegations in paragraphs 1 – 97 in this Complaint, as if fully alleged herein.

116. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

1 117. An actual controversy has arisen in the wake of the Data Breach
2 regarding Aeries' present and prospective common law and other duties to reasonably
3 safeguard its users' PII, and whether Aeries is currently maintaining data security
4 measures adequate to protect Plaintiffs and class members from further data breaches
5 that compromise their PII. Plaintiffs and class members remain at imminent risk that
6 further compromises of their PII will occur in the future. This is true even if they are
7 not actively using Aeries' products or services.

8 118. Pursuant to its authority under the Declaratory Judgment Act, this Court
9 should enter a judgment declaring, among other things, the following:

- 10 a. Aeries continues to owe a legal duty to secure users' PII and to timely
11 notify consumers of a data breach under the common law, Section 5 of
12 the FTC Act, the CCPA, and various state statutes;
- 13 b. Aeries continues to breach this legal duty by failing to employ reasonable
14 measures to secure Plaintiffs and class members' PII.

15 119. The Court also should issue corresponding prospective injunctive relief
16 pursuant to 28 U.S.C. §2202, requiring Aeries to employ adequate security practices
17 consistent with law and industry standards to protect its users' PII.

18 120. If an injunction is not issued, Plaintiffs and class members will suffer
19 irreparable injury, and lack an adequate legal remedy, in the event of another data
20 breach of Aeries. The risk of another such breach is real, immediate, and substantial.
21 If another breach occurs, Plaintiffs and class members will not have an adequate
22 remedy at law because many of the resulting injuries are not readily quantified and they
23 will be forced to bring multiple lawsuits to rectify the same conduct.

24 121. The hardship to Plaintiffs and class members if an injunction does not
25 issue exceeds the hardship to Aeries if an injunction is issued. Among other things, if
26 another data breach occurs at Aeries, Plaintiffs and class members will likely be
27 subjected to fraud, identity theft, and other harms described herein. On the other hand,
28

1 the cost to Aeries of complying with an injunction by employing reasonable
 2 prospective data security measures is relatively minimal, and Aeries has a pre-existing
 3 legal obligation to employ such measures.

4 122. Issuance of the requested injunction will not disserve the public interest.
 5 To the contrary, such an injunction would benefit the public by preventing another
 6 data breach at Aeries, thus eliminating additional injuries that would result to Plaintiffs,
 7 class members, and the hundreds of thousands of students and guardians whose PII
 8 would be further compromised.

9 10 **Count 3**

11 **BREACH OF CONFIDENCE**

12 **Against Aeries on Behalf of Individual Plaintiffs and Class Plaintiff and the Class**

13 123. Plaintiffs repeat the allegations in paragraphs 1 – 97 in this Complaint, as
 14 if fully alleged herein.

15 124. Plaintiffs D.G. and V.G. and the minor class members are a particularly
 16 vulnerable and defenseless group of Aeries users and are more significantly damaged
 17 and imminently threatened to be damaged as a result of Aeries' breach of confidence
 18 described herein because, without limitation, they are especially: (1) attractive targets
 19 to cyber criminals; (2) vulnerable to fraudulent activity and identity theft with respect
 20 to their stolen PII; (3) defenseless to protect themselves from such theft, fraud, or
 21 identity theft; and (4) subject to prolonged surreptitious fraud and identity theft
 22 following the theft of their data, all of which is well documented in academic and
 23 government-issued materials, by experts in the field, and by the media.

24 125. At all times during Plaintiffs' and class members' interactions with Aeries,
 25 Aeries was fully aware of the confidential and sensitive nature of Plaintiffs' and class
 26 members' PII.

1 126. As alleged herein and above, Aeries' relationship with Plaintiffs and class
2 members was governed by terms and expectations that Plaintiffs' and class members'
3 PII would be collected, stored, and protected in confidence, and would not be
4 disclosed to the public or any unauthorized third parties.

5 127. Plaintiffs and class members provided their respective PII, which was
6 both confidential and novel, to Aeries with the explicit and implicit understandings
7 that Aeries would protect and not permit their PII to be disseminated to the public or
8 any unauthorized parties.

9 128. Plaintiffs and class members also provided their respective PII to Aeries
10 with the explicit and implicit understandings that Aeries would take precautions to
11 protect the PII from unauthorized disclosure, such as following basic principles of
12 encryption and information security practices.

13 129. Aeries voluntarily received in confidence Plaintiffs' and class members'
14 PII with the understanding that PII was confidential and novel and, as such, would
15 not be disclosed or disseminated to the public or any unauthorized third parties.

16 130. Due to Aeries' failure to prevent, detect, and avoid the Data Breach from
17 occurring by following best information security practices to secure Plaintiffs' and class
18 members' PII, Aeries caused Plaintiffs' and class members' PII to be disclosed and
19 misappropriated to the public and unauthorized third parties beyond Plaintiffs' and
20 class members' confidence, and without their express permission.

21 131. But for Aeries' disclosure of Plaintiffs' and class members' PII in
22 violation of the parties' understanding of confidence, their PII would not have been
23 compromised, stolen, viewed, accessed, and/or used by unauthorized third parties.
24 The Data Breach was the direct and legal cause of the theft of Plaintiffs' and class
25 members' PII, as well as the resulting damages.

26 132. The injury and harm Plaintiffs and class members suffered was the
27 reasonably foreseeable result of Aeries' unauthorized disclosure of Plaintiffs' and class
28

1 members' PII. Aeries knew its computer systems and technologies for accepting,
2 securing, and storing Plaintiffs' and class members' PII had serious security
3 vulnerabilities because Aeries failed to observe even basic information security
4 practices or correct known security vulnerabilities.

5 133. As a direct and proximate result of Aeries' breaches of confidence,
6 Plaintiffs and class members have been injured and were damaged as discussed herein
7 and as will be proven at trial.

8 134. Moreover, Plaintiffs D.G. and V.G. and the class members that are
9 minors are a particularly vulnerable and defenseless group of Aeries' users and are
10 more significantly damaged and imminently threatened to be damaged as a result of
11 Aeries' breach of confidence described herein.

12 135. As a direct and proximate result of Aeries' breach of confidence,
13 Plaintiffs and class members have been injured and are entitled to damages in an
14 amount to be proven at trial. Such injuries include one or more of the following:
15 ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other
16 misuse, resulting in monetary loss and economic harm; actual identity theft crimes,
17 fraud, and other misuse, resulting in monetary loss and economic harm; loss of the
18 value of their privacy and the confidentiality of the stolen PII; illegal sale of the
19 compromised PII on the black market; mitigation expenses and time spent on credit
20 monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in
21 response to the Data Breach investigating the nature of the Data Breach not fully
22 disclosed by Aeries, reviewing bank statements, payment card statements, and credit
23 reports; expenses and time spent initiating fraud alerts; decreased credit scores and
24 ratings; lost work time; lost value of the PII; lost benefit of their bargains and
25 overcharges for services; and other economic and non-economic harm.

1 **Count 4**

2 **BREACH OF CONTRACT**

3 **Against Aeries on Behalf of Individual Plaintiffs and Class Plaintiff and the Class**

4 136. Plaintiffs repeat the allegations in paragraphs 1 – 97 in this Complaint, as
5 if fully alleged herein.

6 137. Aeries' Privacy Policy (the "Privacy Policy") is an agreement between
7 Aeries and its school district customers. Plaintiffs and class members are the clear
8 intended third-party beneficiaries of the Privacy Policy.

9 138. The Privacy Policy states that it applies to persons "using Aeries
10 products," and it details how Aeries will both protect and use the PII provided by users
11 of Aeries' products and services, including PII stored on or processed through Aeries'
12 databases and systems that was provided by its school district clients (and their
13 component educational institutions).

14 139. The Privacy Policy provides detailed information about what types of PII
15 will be shared and with what entities. It further promises that Aeries "takes various
16 security measures—physical, electronic, and procedural—to help defend against the
17 unauthorized access and disclosure of your information," that its "employees are
18 required to comply with information security safeguards," and that its "systems are
19 protected by technological measures to help prevent unauthorized individuals from
20 gaining access."

21 140. Aeries' school district clients on the one hand and Aeries on the other
22 formed a contract pursuant to the Privacy Policy when those school district clients
23 used Aeries products and services for the school districts' students, staff, and students'
24 guardians. Plaintiff and class members became the intended third-party beneficiaries
25 of a direct and substantial benefit under said Privacy Policy contract when they
26 provided PII to Aeries subject to the Privacy Policy. The clear or manifest intent of
27 Aeries and its school district clients to benefit Plaintiffs and class members—e.g.,
28

1 through the protection of their PII that was stored or processed by Aeries in
 2 accordance with the terms of the Privacy Policy--is evidenced by references in the
 3 Privacy Policy to its applicability to Plaintiff and class members' PII, including in those
 4 portions of the Privacy Policy referenced in Paragraphs 26 through 28 of this
 5 Complaint.

6 141. Plaintiffs and class members are entitled to enforce the Privacy Policy
 7 contract as third-party beneficiaries.

8 142. Aeries breached the Privacy Policy contract, to the detriment of Plaintiffs
 9 and class members, by failing to protect their PII. Specifically, Aeries (1) failed to use
 10 reasonable measures to protect that information; and (2) disclosed that information to
 11 unauthorized third parties, in violation of the agreement.

12 143. As a direct result of Aeries' breach of contract, Plaintiffs and the Class
 13 have suffered injury, have been damaged as described herein and as will be proven at
 14 trial, and are entitled to damages in an amount to be proven at trial.

15 **Count 5**

16 **CALIFORNIA'S UNFAIR COMPETITION LAW**

17 *Cal. Bus. & Prof. Code §§ 17200, et seq.*

18 Against Aeries on Behalf of Individual Plaintiffs and Class Plaintiff and the Class

19 144. Plaintiffs repeat the allegations in paragraphs 1 – 97 in this Complaint, as
 20 if fully alleged herein.

21 145. Aeries is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

22 146. Aeries violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by
 23 engaging in unlawful, unfair, and deceptive business acts and practices.

24 147. Aeries' unfair acts and practices include:

- 25 a. Aeries failed to implement and maintain reasonable security measures to
- 26 protect Plaintiffs' and class members' PII from unauthorized disclosure,
- 27 release, data breaches, and theft, which was a direct and proximate cause

1 of the Data Breach. Aeries failed to identify foreseeable security risks,
 2 remediate identified security risks, and adequately improve security
 3 following previous cybersecurity incidents in the education sector. This
 4 conduct, with little if any utility, is unfair when weighed against the harm
 5 to Plaintiffs and class members whose PII has been compromised.

6 b. Aeries' failure to implement and maintain reasonable security measures
 7 also was contrary to legislatively declared public policy that seeks to
 8 protect consumers' data and ensure that entities that are trusted with it
 9 use appropriate security measures. These policies are reflected in laws,
 10 including the FTC Act, 15 U.S.C. § 45, California's Consumer Records
 11 Act, Cal. Civ. Code §§ 1798.81.5 *et seq.*, and California's Consumer
 12 Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.*

13 c. Aeries' failure to implement and maintain reasonable security measures
 14 also lead to substantial consumer injuries, as described above, that are not
 15 outweighed by any countervailing benefits to consumers or competition.
 16 Moreover, because consumers could not know of Aeries' inadequate
 17 security, consumers could not have reasonably avoided the harms that
 18 Aeries caused.

19 d. Engaging in unlawful business practices by violating Cal. Civ. Code
 20 § 1798.82.

21 148. Aeries has engaged in "unlawful" business practices by violating multiple
 22 laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5
 23 (requiring reasonable data security measures) and 1798.82 (requiring timely breach
 24 notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et*
 25 *seq.*, the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code
 26 §§ 1798.100, *et seq.*, and California common law.

27 149. Aeries' unlawful, unfair, and deceptive acts and practices include:
 28

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and class members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the education sector, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and class members' PII, including by implementing and maintaining reasonable security measures
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.*
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and class members' PII; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45; California's Customer Records

1 Act, Cal. Civ. Code §§ 1798.80, *et seq.*; and California's Consumer Privacy
2 Act, Cal. Civ. Code §§ 1798.100 *et seq.*

3 150. Aeries' representations and omissions were material because they were
4 likely to deceive reasonable consumers about the adequacy of Aeries' data security and
5 ability to protect the confidentiality of consumers' PII.

6 151. Aeries intended to mislead Plaintiffs and class members and induce them
7 to rely on its misrepresentations and omissions.

8 152. Had Aeries disclosed to Plaintiffs and class members that its data systems
9 were not secure and, thus, vulnerable to attack, Aeries would have been unable to
10 continue in business and it would have been forced to adopt reasonable data security
11 measures and comply with the law. Instead, Aeries received, maintained, and compiled
12 Plaintiffs' and class members' PII as part of the services Aeries provided and for which
13 its school district customers (and through them Plaintiffs class members) paid without
14 advising its school district customers, Plaintiffs, and class members that Aeries' data
15 security practices were insufficient to maintain the safety and confidentiality of
16 Plaintiffs' and class members' PII. Accordingly, Plaintiffs and class members acted
17 reasonably in relying on Aeries' misrepresentations and omissions, the truth of which
18 they could not have discovered.

19 153. Aeries acted intentionally, knowingly, and maliciously to violate
20 California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and class
21 members' rights. Past breaches within the education sector put Aeries on notice that
22 its security and privacy protections were inadequate.

23 154. As a direct and proximate result of Aeries' unfair, unlawful, and
24 fraudulent acts and practices, Plaintiffs and class members have suffered and will
25 continue to suffer injury, ascertainable losses of money or property, and monetary and
26 non-monetary damages as described herein and as will be proved at trial. These losses
27 include the diminished value of Plaintiffs' and class members' PII. Because the integrity
28

1 of Plaintiffs' PII is crucial to their future ability to engage in many aspects of
 2 commerce, including obtaining a mortgage, credit card, business loan, tax return, or
 3 even applying for a job, the diminishment of the integrity of that PII corresponds to a
 4 diminishment in value. In other words, Plaintiffs have both a present or future
 5 property interest diminished as a result of Aeries' unfair, unlawful, and fraudulent acts
 6 and practices.

7 155. Plaintiffs and class members seek all monetary and non-monetary relief
 8 allowed by law, including restitution of all profits stemming from Aeries' unfair,
 9 unlawful, and fraudulent business practices or use of their PII; declaratory relief;
 10 reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5;
 11 injunctive relief; and other appropriate equitable relief.

12 156. As child victims, Plaintiffs D.G. and V.G. and minor class members have
 13 suffered greater harm from Aeries' violation of the California Unfair Competition Law
 14 than adult victims.

15 **Count 6**

16 **CALIFORNIA CUSTOMER RECORDS ACT**

17 *Cal. Civ. Code §§ 1798.80, et seq.*

18 Against Aeries on Behalf of Individual Plaintiffs and Class Plaintiff and the Class

19 157. Plaintiffs repeat the allegations in paragraphs 1 – 97 in this Complaint, as
 20 if fully alleged herein.

21 158. “[T]o ensure that Personal Information about California residents is
 22 protected,” the California legislature enacted Cal. Civ. Code § 1798.81.5, which
 23 requires that any business that “owns, licenses, or maintains Personal Information
 24 about a California resident shall implement and maintain reasonable security
 25 procedures and practices appropriate to the nature of the information, to protect the
 26 Personal Information from unauthorized access, destruction, use, modification, or
 27 disclosure.”

1 159. Aeries is a business that maintains Personal Information, within the
2 meaning of Cal. Civ. Code § 1798.81.5, about Plaintiffs and California Subclass and
3 California Minor Subclass members.

4 160. Businesses that maintain computerized data that includes Personal
5 Information are required to “notify the owner or licensee of the information of the
6 breach of the security of the data immediately following discovery, if the personal
7 information was, or is reasonably believed to have been, acquired by an unauthorized
8 person.” Cal. Civ. Code § 1798.82(b). Among other requirements, the security breach
9 notification must include “the types of Personal Information that were or are
10 reasonably believed to have been the subject of the breach.” Cal. Civ. Code § 1798.82.

11 161. Aeries is a business that maintains computerized data that includes
12 Personal Information as defined by Cal. Civ. Code § 1798.80.

13 162. Plaintiffs’ and the class members’ Personal Information includes
14 Personal Information as covered by Cal. Civ. Code § 1798.82.

15 163. Because Aeries reasonably believed that Plaintiffs’ and the class
16 members’ Personal Information was acquired by unauthorized persons during the
17 Data Breach, Aeries had an obligation to disclose the full scope of the Data Breach
18 immediately following its discovery to the owners or licensees of the Personal
19 Information (i.e., Aeries’ school district customers), as mandated by Cal. Civ. Code
20 § 1798.82. Indeed, Aeries’ own privacy policy states that it would provide affected
21 individuals with notice of a data breach.

22 164. By failing to disclose the Data Breach (or its full scope) immediately
23 following its discovery, Aeries violated Cal. Civ. Code § 1798.82. Aeries’ failure to
24 timely and accurately notify its school district customers caused harm to Plaintiffs, who
25 received an even more delayed and inaccurate notification.

1 170. Plaintiffs’ and the class members’ PII is “nonencrypted and nonredacted
2 personal information” as that term is used in Cal. Civ. Code § 1798.150(a)(1). At a
3 minimum, this PII included the individual’s first name or first initial and last name, in
4 combination with medical information and health insurance information. In some
5 instances, the PII also included social security numbers, financial information, and
6 unique identification numbers issued on government documents (e.g., driver’s license
7 number, California identification card number, etc.).

8 171. The Data Breach constitutes “an unauthorized access and exfiltration,
9 theft, or disclosure” pursuant to Cal. Civ. Code § 1798.150(a)(1).

10 172. Aeries had a duty to implement and maintain reasonable security
11 procedures and practices appropriate to the nature of the Plaintiffs’ and class members’
12 PII to protect said PII.

13 173. Aeries breached the duty it owed to Plaintiffs and California Subclass
14 Members described above, including the heightened duty owed to Plaintiffs D.G. and
15 V.G. and the class members. Aeries breached these duties by, among other things,
16 failing to: (a) exercise reasonable care and implement adequate security systems,
17 protocols and practices sufficient to protect the PII of Plaintiffs and class members;
18 (b) detect the breach while it was ongoing; and (c) maintain security systems consistent
19 with industry standards.

20 174. Aeries’ breach of the duty it owed to Plaintiffs and class members was
21 the direct and proximate cause of the Data Breach. As a result, Plaintiffs and class
22 members suffered damages, as described above and as will be proven at trial.

23 175. Plaintiffs seek injunctive relief in the form of an order enjoining Aeries
24 from continuing the practices that constituted its breach of the duty owed to Plaintiffs
25 and class members as described above. Because Plaintiffs also served a letter of notice
26 on Aeries pursuant to Cal. Civ. Code § 1798.150(b), and Aeries did not provide a
27 response indicating that it had cured the theft of Plaintiffs’ PII, Plaintiffs further seek
28

1 statutory damages not less than \$100 and not greater than \$750, or actual damages, for
2 each member of the class.

3 **REQUEST FOR RELIEF**

4 **WHEREFORE**, Individual Plaintiffs and Class Plaintiff, individually and on
5 behalf of all class members proposed in this Complaint, respectfully request that the
6 Court enter judgment in their favor and against Aeries as follows:

- 7 1) For an Order certifying the class, as defined herein, and appointing Class
8 Plaintiff and Plaintiffs' counsel to represent the class as alleged herein;
- 9 2) For injunctive and other equitable relief as is necessary to protect the interests
10 of Plaintiffs and class members, including but not limited to an order:
- 11 a) Prohibiting Aeries from engaging in the wrongful and unlawful acts
12 described herein;
- 13 b) Requiring Aeries to protect, including through adequate encryption, all data
14 collected through the course of its business in accordance with all applicable
15 regulations, industry standards, and federal, state, or local laws;
- 16 c) Requiring Aeries to delete, destroy, and purge the PII of Plaintiffs and class
17 members unless Aeries can provide the Court a reasonable justification for
18 the retention and use of such information when weighed against the privacy
19 interests of Plaintiffs and the class members;
- 20 d) Requiring Aeries to implement and maintain a comprehensive Information
21 Security Program designed to protect the confidentiality and integrity of
22 Plaintiffs' and class members' PII;
- 23 e) Requiring Aeries to engage independent third-party security auditors and
24 internal personnel to run automated security monitoring;
- 25 f) Requiring Aeries to audit, test, and train its personnel regarding any new or
26 modified procedures;
- 27
28

- g) Requiring Aeries to segment data by, among other things, creating firewalls and access controls so that if one area of Aeries' network is compromised, hackers cannot gain access to other portions of Aeries' systems;
- h) Requiring Aeries to conduct regular database scanning and security checks;
- i) Requiring Aeries to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and class members;
- j) Requiring Aeries to routinely and continually conduct internal training and education, at least annually, to inform security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- k) Requiring Aeries to implement, maintain, regularly review, and revise as necessary, a threat management program designed to appropriately monitor Aeries' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- l) Requiring Aeries to meaningfully educate all class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;
- m) Requiring Aeries to implement logging and monitoring programs sufficient to track traffic to and from its servers, as well as programs sufficient to protect infiltration of school districts' local servers connected to Aeries' systems; and
- n) Requiring Aeries to provide ten years of identity theft and fraud protection services to Plaintiffs and class members.

- 3) For an award of compensatory, consequential, and general damages, including nominal damages, as allowed by law in an amount to be determined;
- 4) For an award of statutory damages and punitive damages, as allowed by law in an amount to be determined;
- 5) For an award of restitution or disgorgement, in an amount to be determined;
- 6) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- 7) For prejudgment interest on all amounts awarded; and
- 8) Such other and further relief as the Court may deem just and proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and the Class of all others similarly situated, hereby demand a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: June 8, 2021

Respectfully submitted,

/s/ Daniel L. Warshaw

Daniel L. Warshaw (CA Bar No. 185365)

**PEARSON, SIMON &
WARSHAW, LLP**

15165 Ventura Boulevard, Suite 400

Sherman Oaks, CA 91403

Telephone: (818) 788-8300

Facsimile: (818) 788-8104

Email: dwarshaw@pswlaw.com

Hassan A. Zavareei (CA Bar No. 181547)

TYCKO & ZAVAREEI LLP

1828 L Street NW, Suite 1000

Washington, D.C. 20036

Telephone: (202) 973-0900

Facsimile: (202) 973-0950

Email: hzavareei@tzlegal.com

Counsel for Plaintiffs and the Proposed Class

Exhibit A

From: **ABC Unified School District via Aeries Communication** <17887785-do-not-reply@a.signalkit.com>

Date: Wed, May 13, 2020 at 5:23 PM

Subject: Notice of Data Breach

To: <naarayan@gmail.com>



NOTICE OF DATA BREACH

The District's Information & Technology department has received notification from **Aeries Software Inc**, our database vendor, that the District's student information system database was compromised through a vulnerability in the Aeries software. We are currently investigating this issue.

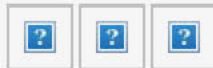
Until we know the extent of this possible breach, we need all ABC students and families with Aeries portal accounts to reset their passwords.

Tomorrow, May 14, 2020, an email will be sent to all ABC parent/student account holders with a link to reset their password.

Once we have more information, families impacted will be notified by the District.

Thank you,

Dr. Colin Sprigg
Director
Information & Technology



You are receiving this email because your email address is associated with
ABC Unified School District
16700 Norwalk Blvd. Cerritos, CA 90703

Want to change how you receive these emails?

[Manage your notification preferences](#)

[You've contacted the wrong person](#)

Copyright © 2019

Exhibit B

From: **Colin Sprigg via Aeries Communication** <17896938-do-not-reply@a.signalkit.com>
Date: Thu, May 14, 2020 at 6:37 PM
Subject: An announcement from Colin Sprigg (Aeries Portal Password Reset)
To: <naarayan@gmail.com>

Dear ABC Parents and Students that have an Aeries Portal account:

As published within ABC Unified's **Notice of Data Breach** shared with the ABC community on May 13 (see attached), the school district will require all ABC parents and students that have an online Aeries Portal account to reset their passwords for security purposes. Please follow the written instructions below to manually reset your passwords. All Aeries Portal functions will not be accessible beginning May 14 until this process has been completed.

Password Reset Instructions

- Go to <https://parentportal.abcusd.us>
- Click on **Forgot Password?**
- Type the email address for your Parent Portal account

(Click **Next**)

- Check your email inbox for a message from portal.confirmation@abcusd.us
- Open the message and click on the link that says **Click Here**
- Click **Next**
- Enter your new password in both the **New Password** field and again in the **ReType New Password** field. (Click **Next**)
- Once you see the screen that says **Complete**, the password reset process is done.

For more information go to the ABC Unified School District website at www.abcusd.us > **Departments > Information and Technology > Data Breach.**

For technical support, please review the attached password reset “how-to” document, or contact the Online Learning at Home Technical Support Line at (562) 229-7929 from 8:30 AM to 4 PM, or email support@abcusd.us.

Thank you,
Dr. Colin Sprigg, Director
Information and Technology

This announcement included a file attachment. Click the link below to view.

[How to Reset your Parent Portal Account Password.pdf](#)
[Data_Breach_05.13.20_v1.pdf](#)



You are receiving this email because your email address is associated with
ABC Unified School District
16700 Norwalk Blvd. Cerritos, CA 90703

Want to change how you receive these emails?

[Manage your notification preferences](#)

[You've contacted the wrong person](#)

Copyright © 2019

Exhibit C

From: **Colin Sprigg via Aeries Communication** <18038891-do-not-reply@a.signalkit.com>
Date: Thu, May 28, 2020 at 1:34 PM
Subject: An announcement from Colin Sprigg
To: <Naarayan@gmail.com>

Dear ABC Community:

On May 13, the ABC Unified School District publicly reported that a software data breach had occurred involving Aeries Portal, the online program allowing student and parent access to common educational records. In order to keep all ABC Aeries Portal users secure, the District revoked all Aeries Portal passwords, requiring all account holders to manually reset their passwords to regain access.

The District has since learned which ABC families were affected by the breach, and this notice serves to more

fully inform those impacted of what data was compromised, the District's response, and what families can do to further protect their information.

This notice is publicly posted on the District website at www.abcusd.us > Departments > Information and Technology.

Notice of Data Breach	
What Happened?	<p>On May 12, 2020, the ABC Unified School District was informed by Aeries Software, Inc., the vendor for our student information database, that they had suffered a data breach impacting those who use the ABC USD portal.</p> <p>State and federal law enforcement agencies are conducting ongoing investigations into this data breach. At this point, investigators believe one entity was responsible for the attack, and suspects are in custody.</p> <p>Aeries Software has since patched the software issue that allowed unauthorized access to occur.</p>
What Information was Involved?	<p>The following information was exposed on November 4, 2019:</p> <ul style="list-style-type: none"> • Parent Name • Student Name • Student ID (School) • Physical Resident Address

	<p>Email Address</p> <ul style="list-style-type: none"> <p>Password “hashes” Aeries automatically encrypts passwords. A password hash does not reveal the password. However, with access to a password hash, unauthorized persons may be able to deconstruct weak, common, or simple passwords.</p> <p><u>No other information was exposed.</u> No social security numbers are maintained in the Aeries system; therefore, no risk of compromise to this data is possible.</p> <p>ABC has determined that the unauthorized party attempted to gather your information. No evidence exists that your data was taken, nor misused. ABC is required by law to notify the families that were subject to unauthorized access.</p>
What the District is Doing.	ABCUSD Information & Technology revoked all existing passwords, and users were instructed on how to manually reset their password.
What You Need to Do.	<p>Parents and students need to reset their Aeries Portal password in response to this incident before further access is granted.</p> <p>It is recommended that families consider changing user names, and/or passwords that may have been in common with those used with the Aeries Portal.</p>
<p>For additional support, please contact the Tech Support Hotline at (562) 229-7929.</p>	



You are receiving this email because your email address is associated with
ABC Unified School District
 16700 Norwalk Blvd. Cerritos, CA 90703

Want to change how you receive these emails?

[Manage your notification preferences](#)
[You've contacted the wrong person](#)

Copyright © 2019

Exhibit D

San Dieguito Union High School District - Notice Of Data Breach

NEWS PROVIDED BY


San Dieguito Union High School District →

May 14, 2020, 21:00 ET

ENCINITAS, Calif., May 14, 2020 /PRNewswire/ -- Although it has no confirmation that personal information was acquired without authorization, San Dieguito Union High School District ("SDUHSD") announced today that it has taken action after becoming aware of an incident in which an unknown third party gained access to certain employee email accounts. Out of an abundance of caution, SDUHSD is providing notice of this event to potentially impacted individuals as well as certain regulators.

What Happened? SDUHSD became aware of unusual activity related to certain employees' email accounts. SDUHSD immediately launched an investigation, with the aid of forensic experts, to determine the nature and the scope of the activity. SDUHSD learned of unauthorized access to certain employees' email accounts. The unauthorized access occurred between July 1, 2019 to July 17, 2019. SDUHSD undertook a lengthy and labor-intensive process to identify the personal information contained in the affected email accounts. Since SDUHSD confirmed the individuals impacted by this event, SDUHSD has worked to obtain mailing addresses for the impacted individuals where possible. While the investigation was unable to determine the scope of information that was actually accessed within the affected email accounts, SDUHSD is notifying potentially affected individuals in an abundance of caution.

What Information Was Involved? While SDUHSD was unable to confirm whether any information was accessed or acquired by the unauthorized individual, the investigation confirmed that the following types of information were present in the affected email accounts: name, address, Social Security number, driver's license/state identification number, passport number, financial account number, diagnosis information, medical information, health



What We Are Doing. SDUHSD takes this incident and the security of personal information in their care very seriously. SDUHSD has security measures in place to protect the data on their systems and they continue to assess and update security measures and training to their employees to safeguard the privacy and security of information in their care. As an added precaution, SDUHSD is offering affected individuals access to credit monitoring and identity protection services at no cost. Because SDUHSD has insufficient contact information for some of the individuals whose information may be contained in the affected email accounts, it is providing notice to potentially impacted individuals by way of a notification published to certain state media outlets. SDUHSD is mailing notice letters to those individuals for whom it has confirmed mailing address information. SDUHSD is also notifying regulatory authorities, as required by law.

For More Information. Individuals who may have questions about the incident, may contact our dedicated call center at 1-844-963-2715 Monday through Friday from 8:00 a.m. to 5:30 p.m. CT, or visit SDUHSD's website at sduhsd.net.

What You Can Do. SDUHSD encourages individuals to remain vigilant against incidents of identity theft and fraud, to review their account statements, and to monitor their credit reports for suspicious activity. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report.

Individuals have the right to place a "security freeze" on their credit report, which will prohibit a consumer reporting agency from releasing information in their credit report without an individual's expressed authorization. The security freeze is designed to prevent credit, loans, and services from being approved in an individual's name without their consent. However, individuals should be aware that using a security freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or applications made regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, individuals cannot be charged to place or lift a security freeze on their credit

report. Should individuals wish to place a security freeze, please contact the major consumer reporting agencies listed below:

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

In order to request a security freeze, individuals will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
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.

As an alternative to a security freeze, individuals have the right to place an initial or extended "fraud alert" on their file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If an individual is a victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should individuals wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services



Individuals can further educate themselves regarding identity theft, fraud alerts, security freezes, and the steps they can take to protect themselves by contacting the consumer reporting agencies, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Individuals can obtain further information on how to file such a complaint by way of the contact information listed above. Individuals have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, individuals will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and individuals' state Attorney General. This notice has not been delayed by law enforcement.

SOURCE San Dieguito Union High School District

Related Links

<http://sduhsd.net>