SKLAR WILLIAMS PLLC
Stephen R. Hackett, Esq., NSBN: 5010
Johnathon Fayeghi, Esq., NSBN: 12736
Matthew S. Fox, Esq., NSBN: 12884
David B. Barney, Esq., NSBN: 14681
410 South Rampart Boulevard, Suite 350
Las Vegas, Nevada 89145
Telephone: (702) 360-6000
Facsimile: (702) 360-0000
Email: shackett@sklar-law.com
jfayeghi@sklar-law.com
mfox@sklar-law.com
dbarney@sklar-law.com

WHATLEY KALLAS, LLP
Alan M. Mansfield, Esq.*
16870 W. Bernardo Drive, Suite 400
San Diego, CA 92127
Telephone: (619) 308-5034
Facsimile: (888) 341-5048
Email: amansfield@whatleykallas.com

DOYLE APC
William J. Doyle, Esq.*
550 West B Street, 4th Floor
San Diego, CA 92101
Telephone: (619) 736-0000
Facsimile: (619) 736-1111
Email: bill@doyleapc.com

And additional counsel named below

Attorneys for Plaintiffs and the Class

CASE NO: A-23-880643-C
Department 6

DISTRICT COURT

CLARK COUNTY, NEVADA

JANE DOE, on behalf of her minor child JOHN DOE and all others similarly situated; and ERIN TIMRAWI, on behalf of herself and all others similarly situated,

Plaintiffs,

vs.

CLARK COUNTY SCHOOL DISTRICT, a political subdivision of the State of Nevada; DOES 1 through 10, inclusive; and ROE ENTITIES I through X, inclusive,

Defendants.

CASE NO.:
DEPT. NO.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

ARBITRATION EXEMPTION:
(1) Class Action, and (2) Action Seeking Equitable Relief

Plaintiffs JANE DOE[1] and ERIN TIMRAWI (collectively, "Plaintiffs"), by and through undersigned counsel, hereby file this action in the capacities referenced above and on behalf of all others similarly situated, against the CLARK COUNTY SCHOOL DISTRICT ("CCSD" or the "District"), DOES 1–10, inclusive, and ROE ENTITIES I through X, inclusive (collectively, "Defendants"), and allege the following based on personal knowledge as to the allegations regarding themselves, and upon information and belief as to all other allegations:

SUMMARY OF THE ACTION

1. In early October 2023 (and possibly earlier), CCSD was subject to a ransomware attack and accompanying data breach and theft, which led to the compromise and public release of highly sensitive information belonging to CCSD's teachers, students, their families, and even students who previously graduated from schools in the District. This action arises from the negligent and/or reckless failure by CCSD to adequately protect such private, personal, financial, and medical information from being obtained, viewed, compromised, and/or disclosed by third parties.

2. Plaintiffs bring this action in their stated capacities and on behalf of all individuals comprising the Class (defined below), to ensure that CCSD takes steps necessary to rectify its failures and secure the information of its students, parents, and teachers going forward.

3. CCSD abdicated its obligation and duty to protect sensitive personal information in its possession, as described in further detail below, and failed to take steps necessary to prevent a sweeping attack that compromised the privacy and security of that data. Based on information available to CCSD, and in view of the known threat of recent cyber-attacks against school systems, this was an entirely foreseeable event that could and should have been prevented but was not, due to the negligent design of CCSD's network and the failure to have in place controls and software protections that would identify and/or alert CCSD of an attack, or even prevent an attack in the first place. School districts throughout Nevada and the United States have been warned repeatedly

[1] Due to the sensitive nature of this action and to protect the safety of a minor child, Plaintiff Jane Doe has chosen to file this action under pseudonyms for herself and her minor child, John Doe. *See Does v. Advanced Textile Corp.*, 214 F.3d 1058, 1068-69 (9th Cir. 2000).

of the potential for such an attack on their computer systems, and several school districts in Nevada—**including CCSD itself on August 27, 2020**, and Washoe County School District in 2019—had already been the subject of such attacks.

4. Rather, in acts of recklessness and in violation of numerous regulations and standards, it appears CCSD failed to implement reasonable and adequate security procedures to protect this data, failed to update software licenses, failed to have in place software protections that would identify and/or alert CCSD of an attack or prevent such an attack in the first place, and failed to put into place common password protections to prevent hacking of accounts, including requiring multi-factor authentication for all user accounts.

5. To date, CCSD has failed and/or refused to fully and adequately notify victims of this attack that their personal information was improperly accessed and stolen, the status of their information, if the District was subject to a ransomware attack, or even the type and extent of information taken about Class members, leaving victims in the dark as to what they can and should do to protect themselves. CCSD also has failed to implement and maintain reasonable security procedures and practices appropriate for the type of information at issue, in order to protect Plaintiffs' and Class members' sensitive personal information or PII. To make matters worse, CCSD has failed to ensure that the third parties responsible for the ransomware attack no longer have access to the District's computer networks, approximately one month after CCSD was advised the attack had occurred.

6. CCSD disclosed or permitted the disclosure of Plaintiffs' and Class members' sensitive personal information or PII to unauthorized persons. Defendants and their responsible contractors, subcontractors, representatives and/or employees negligently, recklessly, wantonly, or consciously created, maintained, preserved, and/or stored Plaintiffs' and Class members' individual personally identifiable information, including "personal information" within the meaning of NRS 603A.040, on an inadequately protected network. CCSD further failed to maintain the confidentiality of records containing Plaintiffs' and Class members' personal information and failed to implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

7. These actions proximately resulted in damages and loss to Plaintiffs and Class members, as their medical, financial, and/or other personal information was improperly accessed and exfiltrated by unauthorized third parties.

8. "PII," for purposes of this Complaint, refers to sensitive personal information including, but not limited to, name, date of birth, ethnicity, medical information, financial information, student behavioral information, cyber-bullying information, student records, employee records, and health insurance information. The term also includes information identified in NRS 603A.040, including a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: Social Security number, driver's license number, driver authorization card number or identification card number, account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account, a medical identification number or a health insurance identification number, or a user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account. Also, it refers to that information identified in NAC 388.076, including student name, name of the student's parent or other family members, the address of the student or student's family, any personal identifier, such as the student's social security number, student number, or biometric record, any other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name, and any other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

/ / /

/ / /

/ / /

9. Given that PII encompasses such personal and revealing information, it is highly valued as a gateway to medical identity theft[2] and general identity theft.[3] PII has been found to command up to $1,000 per individual record on the dark web.[4] Organizations such as CCSD are entrusted with this most sensitive and valuable data. As a result, Defendants have a non-delegable and fiduciary duty to take particularly special care to maintain up-to-date information security practices and keep apprised of industry-related threats as they arise.

10. Public entities and their service provider contractors or subcontractors are legally required and have a non-delegable duty to keep PII in their possession, custody or control private and secured. Defendants breached such duties owed to Plaintiffs and Class members by, *inter alia*, (a) not exercising reasonable care in retaining, maintaining, securing, and safeguarding nonpublic PII from being accessed, stolen, and/or publicly released by unauthorized persons; (b) failing to implement processes to detect a breach or unauthorized access in a timely manner and to act upon any warnings or alerts that Defendants' cybersecurity systems had been breached or improperly accessed; (c) failing to timely disclose the facts surrounding this breach to Plaintiffs and Class members; and (d) failing to disclose that Defendants did not adequately secure Plaintiffs' or Class members' PII.

11. Under the laws set forth herein, Plaintiffs and Class members have a recognized right to confidentiality in their PII and can reasonably expect that their PII would be protected by Defendants from unauthorized access. When Plaintiffs and Class members either directly or on behalf of their dependents provided PII to CCSD for the purpose of employment, enrollment, and otherwise availing themselves of services through CCSD, they did so with the reasonable understanding and assurance that their PII would be kept confidential and secure.

12. Nevada State laws and regulations, as well as Clark County School District

---

[2] R. Kam, *et al*, *Medical Identity Theft: A Deadly Side Effect of Healthcare Data Breaches*, ID Experts (2017).

[3] Identity Theft Resource Center, *Data Breaches in the Healthcare Industry Continue Due to Availability of Valuable Information* (8/11/2020).

[4] M. Yao, *Your Electronic Medical Records Could be Worth $1,000 to Hackers*, Forbes (4/18/17).

Regulations and Policies support these reasonable expectations. For example, NRS 603A.210 requires that data collectors maintain reasonable security measures to protect personal information. NRS 392.029 requires public schools to protect education records from release without written consent. NAC 388.289 requires that confidentiality of personally identifiable information of special education students be protected at its collection, storage, disclosure, and destruction. In addition, Clark County School District Policy 5125 "recognizes the confidential nature of student records." In a related regulation, CCSD Regulation 5125.1, the District states that all school records of students are "confidential" and may only be released to particular individuals upon written request. Similarly, personnel information regarding District employees is also confidential and may only be reviewed on a need-to-know basis. CCSD Regulation 4311. According to District Regulation 1212, "Confidential information concerning all personnel will be safeguarded." Finally, in recognition of the extremely sensitive nature of many of the records held by the District, CCSD specifically promises to protect the privacy of students with diverse gender identities or expressions by not disclosing information that may reveal a student's gender identity or expression status. CCSD Policy 5138. Students receiving special education services with the District also have highly sensitive records the District acknowledges it is required to protect. *See*, CCSD Special Education Procedures Manual, Chapter 10.0.

13. Unfortunately for Plaintiffs and Class members who either are or were enrolled with or employed by CCSD, their PII was not secured in the manner required under Nevada law that would prevent such unauthorized access. Even worse, despite Defendants' obligations under law to promptly notify affected individuals so they can take appropriate action, Defendants have, as of yet, failed to provide the information needed by Plaintiffs and other similarly situated individuals to enable them to react appropriately to the breach, including taking whatever mitigation measures they feel may be necessary. For example, the District has not acknowledged that this was a ransomware attack, that the information is being publicly released, that it includes highly sensitive information, including medical information, or **that the third-parties responsible for the attack may still have access to all of the District's information**. In addition, no formal data breach notice has been provided by the District on its website or specifically to affected

individuals.

14. Defendants disregarded the rights of Plaintiffs and members of the Class by negligently, recklessly, and/or consciously failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class members' PII was safeguarded, failing to take available steps to prevent access to and unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies, and procedures regarding data access and encryption as well as appropriate procedures, such as two-step or multi-factor authentication, which likely would prevent such intrusions. As a result, the PII of at least 200,000 Class members was compromised through disclosure to unauthorized third parties.

15. Plaintiffs and Class members now face a long-term battle against identity theft as a result of this breach. Plaintiffs and Class members have a continuing interest in ensuring that this information is and remains safe. This presents an imminent and impending continuing risk for Plaintiffs and Class members, particularly where CCSD refuses to fully disclose any details of the attack and what data were accessed and were available for third parties to exploit. CCSD's failure to adequately protect the PII in their possession has caused, and will continue to cause, substantial harm and injuries to Plaintiffs and Class members. Plaintiffs and Class members are thus entitled to injunctive and/or other equitable relief.

16. Plaintiffs bring this action seeking damages, injunctive relief, and equitable relief that is appropriate for the benefit of Plaintiffs and Class members, including attorneys' fees, costs and expenses of litigation.

THE PARTIES

17. On personal knowledge, Plaintiff Jane Doe and her minor child John Doe are, and at all times herein relevant were, citizens of the State of Nevada residing in Clark County. John Doe is a minor child enrolled at CCSD as a seventh grade student. During his enrollment at CCSD, John Doe has participated in an Individualized Education Program ("IEP"), a special resource and education plan made available by the District to students with a disability, like John Doe.

18. On personal knowledge, the protection of John Doe's PII from unauthorized disclosure is important and material to him. John Doe was personally impacted and, either directly

or through his guardians, suffered damages as a result of the unauthorized disclosure of personal and/or medical information by CCSD, and the foreseeable and preventable attack on its servers. John Doe and his legal guardians have been forced to spend significant time attempting to address this issue and even to find out if he was a victim of this attack, on top of out-of-pocket costs to monitor the use of his personal information. This, in addition to the fear, anxiety and worry associated with the unauthorized disclosure of his PII, which will be a cause of concern for the rest of John Doe's life. The exfiltration of PII that is associated with John Doe and his family and that was illegally accessed by unauthorized third parties has caused damages as a result of Defendants' misconduct in having John Doe's PII disclosed and stolen without his authorization, and the confidentiality and integrity of his PII breached, lost, not preserved, and not protected. Neither John Doe nor his guardians have received compensation for hours of time and effort required to be expended to date and in the future to address this issue, independent of litigation, as well as spending time and funds in connection with signing up for credit freezes and monitoring. As evidenced by such time and effort required to be spent, John Doe is unable to remedy the impacts of this breach on his own and has no adequate remedy at law.

19. On personal knowledge, Plaintiff Erin Timrawi is, and at all times herein relevant was, a citizen of the State of Nevada residing in Clark County. Plaintiff Erin Timrawi is the mother of a minor child enrolled at CCSD, and her PII was also disclosed without authorization as a result of Defendants' conduct, along with the PII of her child enrolled at CCSD.

20. On personal knowledge, the protection of PII for both Plaintiff Erin Timrawi and her family from unauthorized disclosure is important and material to Plaintiff. Plaintiff Erin Timrawi has experienced fear, anxiety, and worry as a result of the unauthorized disclosure of personal and/or medical information by CCSD since she became aware of it and based on such activity believes that such information would have been viewed and used by third parties without her authorization or consent. She remains concerned about the status of this information as she has not received full and complete notice from CCSD confirming this attack, or the steps she should take to protect both her and her family, particularly in terms of sensitive Social Security numbers and/or PII for both her and her dependents. Plaintiff was personally impacted and

suffered damages as a result of this breach. For example, she has been forced to spend significant time attempting to address this issue and even to find out if she was a victim of this attack, on top of out-of-pocket costs to monitor the use of her personal information and the information of her dependents. The exfiltration of PII that is associated with her and her family and that was illegally accessed by unauthorized third parties has caused damages as a result of Defendants' misconduct in having her PII disclosed to and stolen without her authorization, and the confidentiality and integrity of her PII breached, lost, not preserved, and not protected. Plaintiff has received no compensation for hours of time and effort she had to expend and will be required to expend to address this issue, independent of litigation, as well as spending time and funds in connection with signing up for credit freezes and monitoring. As evidenced by the time and effort she has had to expend, she is unable to remedy the impacts of this breach on her own and has no adequate remedy at law.

21. The PII of Plaintiffs was created, maintained, and preserved by and/or stored on Defendants' computer networks. Such PII included or contained an element of personal identifying information sufficient to allow identification of the individual, such as name, date of birth, address, and Social Security number (which according to Defendants has been compromised), and additionally also would have contained the medical record number, medical benefits paid, insurance provider information, electronic mail address, telephone numbers and/or other information that, alone or in combination with other publicly available information, reveals Plaintiffs' identities.

22. Defendant CCSD is a governmental agency that provides employment, medical, and educational services to residents of Clark County. By acting in such a capacity and collecting PII, CCSD is or should be considered a "covered entity" for purposes of HIPAA and FERPA.

23. The true names and capacities, whether corporate, individual, or otherwise, of Defendant Does 1 through 10, inclusive, and Roe Entities I through X, inclusive, are unknown to Plaintiffs, who therefore sue such Defendants by fictitious names. Each Defendant designated as a Doe and Roe Entity is legally responsible in some manner or means for the damages to Plaintiffs, as alleged herein, either through its contractual duty, conduct, or through the conduct of its agents,

servants, employees or insurers, which resulted in injury and damages to Plaintiffs as alleged herein. Plaintiffs will ask for leave of this Court to amend this Complaint to insert the true names and capacities of said Defendant Does 1 through 10, inclusive, and Roe Entities I through X, inclusive, when the same have been ascertained by Plaintiffs, together with the appropriate charging allegations, and to join said Defendant(s) in this action.

24. Defendants' conduct, as described herein, including reviewing, approving, and/or ratifying the conduct at issue, was undertaken as a supervising agency, agent, and/or servant, and was performed within the course and scope of their oversight authority, agency, or contractor or subcontractor relationship. All Defendants are thus jointly and severally responsible, in whole or in part, for the conduct and injuries alleged herein.

JURISDICTION AND VENUE

25. This Complaint states a controversy over which this Court has jurisdiction and venue is properly in this Court, because the Defendants are residents of Clark County, Nevada, and all of the acts and omissions complained of herein occurred in Clark County, Nevada.

26. The matters in controversy exceed, exclusive of interests and costs, the minimum jurisdictional amount of the Court of Fifteen Thousand Dollars ($15,000.00).

FACTUAL ALLEGATIONS

A. CCSD's Computer Systems are Breached and Significant PII of Students, Parents, and Teachers is Publicly Released.

27. CCSD is the fifth largest school district in the United States, with over 300,000 students and 40,000 employees, including over 18,000 teachers. CCSD has more than 360 schools in the cities of Las Vegas, Henderson, North Las Vegas, and Boulder City.

28. Prior to the ransomware attack at issue, CCSD was well aware of the vulnerabilities of its computer systems. In August 2020, CCSD also experienced a data breach caused by a ransomware attack. Approximately 44,000 people were affected by that attack, and according to national media outlets, the victims' PII was publicly released by the attackers in response to

CCSD's refusal to pay the ransom demand.[5] The attackers had access to CCSD's systems for an entire month, from August 25, 2020, to September 25, 2020. CCSD sent out a formal notice of that data breach 22 days later, on October 16, 2020, identifying that the victims' information potentially had been accessed and acquired in a ransomware attack and offering credit monitoring services to the victims. CCSD was placed on notice by this incident that it should have and could have prevented the instant attack by adequately securing and encrypting the personal information of Plaintiffs and Class members to prevent infiltration by methods such as phishing, credential stuffing, hacking of weak passwords and other known cyber-attack avenues. Defendants failed, however, to take adequate measures to prevent this attack.

29. At the time of CCSD's 2020 data breach, the District stated: "The confidentiality, privacy, and security of information in CCSD's care is one of its highest priorities and CCSD takes this incident very seriously." The District also claimed, "As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures, to implement additional safeguards, and to provide additional training to employees on data privacy and security." According to its 2020 data breach notice, the personal information at issue in that incident included names, dates of birth, addresses, and/or Social Security numbers. CCSD publicly represented it was evaluating its security practices to prevent further attacks. It was also on notice of the inadequacy of its systems and the need to promptly address such inadequacies.

30. Despite the District's statements and prior experience, there is no evidence that CCSD took well-known proactive steps, like requiring multi-factor authentication for all email accounts, having robust password protocols, and implementing all software updates available, to prevent future intrusions despite its public statements and promises. This includes the District's continued practice of requiring its students to use their date of birth as account passwords, and then updating the accounts on an annual basis to use the same passwords year-after-year.

[5] *See* https://www.wsj.com/articles/hacker-releases-information-on-las-vegas-area-students-after-officials-dont-pay-ransom-11601297930 (last visited October 31, 2023).

31. On or about October 5, 2023, CCSD experienced wide-scale cyber-attack, which, upon information and belief, lead to email, Internet, and computer outages, leaving students, staff, and parents in the dark. Weeks after this attack, District representatives still have failed to disclose the nature of the attack, what sensitive information has been stolen, or anything resembling transparent and fulsome notice of this devasting attack, which will have repercussions for its individual victims for years to come.

32. On October 16, 2023, CCSD published the following announcement, but failed to provide any detailed information such as what happened, whether there was a ransomware attack, and what data might have been compromised.

> On approximately October 5, 2023, Clark County School District ("CCSD") became aware of a cybersecurity incident impacting its email environment. Upon discovering the incident, CCSD immediately engaged a team of forensic experts to investigate the incident and ensure that CCSD operates within a safe and remediated email environment. CCSD is also cooperating with law enforcement's investigation.
>
> Thus far, the investigation revealed that the unauthorized party accessed limited personal information related to a subset of students, parents, and employees. CCSD is working diligently to identify all individuals whose information was impacted by this incident. Our comprehensive assessment is ongoing and may span several weeks. Rest assured that we are committed to sharing more information as it becomes available in the coming weeks.
>
> Affected individuals identified by CCSD will receive a notification letter via first-class mail outlining steps to protect their information. No reports of related identity theft since the discovery of the incident have been made to CCSD at this time. The State of Nevada has resources and materials available for those concerned they have been a victim of identity theft.
>
> We understand that you may have questions about this incident that are not addressed in this announcement. If you have additional questions about this incident, please call CCSD's dedicated assistance line at 888-566-5512 between 6:00 a.m. and 6:00 p.m. Pacific Time, Monday through Friday, excluding holidays.

No other details were provided.

33. The CCSD announcement only advises Plaintiffs and Class members that "limited" personal information was "accessed." It did not reveal true extent of the breach nor that the District had been subject to yet another ransomware attack. In fact, contrary to these representations, the PII of over 200,000 people appears to have been stolen by a ransomware group that goes by the

name SingularityMD, which demanded payment that the District refused to make, despite the sensitive nature of the data taken, including medical information. Even more alarming, it appears the hacker group still has access to the District's computer systems, creating an imminent risk of additional breach and disclosure of PII belonging to the District's employees, students, their families, and even past graduates from the District.

34. On October 16, 2023, an email was also sent to parents by the District, which reads, in part, as follows:

> In an effort to safeguard our data and communication, access to Google Workspace will be temporarily limited to the internal CCSD network. Additionally, out of an abundance of caution, we have implemented a forced password change for all students to protect their accounts.
>
> As a result, the school will work with them to change their password, and students will be unable to access Google Workspace, including Gmail and Drive, from outside the CCSD network. Users will have uninterrupted access in schools and administrative buildings.
>
> Students will continue to have access to Canvas and Infinite Campus once their password has been reset.
>
> If you have additional questions about his incident, please call CCSD's dedicated assistance line at 888-566-5512 between 6:00 a.m. and 6:00 p.m. Pacific Time, Monday through Friday, excluding holidays.

35. On October 18, 2023, the District updated its original announcement:

> **October 18, 2023 Update**
>
> CCSD continues working to investigate the cybersecurity incident impacting its email environment. At this time, CCSD employees and students can only access their District email accounts and associated Google Workspace while connected to the District internet.
>
> The District continues working with schools to facilitate password changes for students and staff. While access is limited to Google Workspace, students can still access homework and assignments through Canvas. Parents can continue to email CCSD staff, but for the time being, employees can only respond when on campus.

Notably, this update and CCSD's original announcement minimize and obfuscate the nature of the risk to Plaintiffs and Class Members, by continuing to describe this broad infiltration, access, ransom attack, and exfiltration of PII as a "cybersecurity incident impacting its [CCSD's] email

environment."

36. On October 23, 2023, CCSD published the following update:

> **October 23, 2023 Update**
>
> In alignment with the extension to accommodate challenges related to the requirement for all staff to reset their password, access to the Google Workspace will continue to be limited to the internal CCSD network until Wednesday, October 25, 2023, at 5:00 p.m. Users will continue to have uninterrupted access in schools and administrative buildings. Thank you for your understanding.

37. Two days later, the District published another update, but neither update shed any light for Plaintiffs or Class Members about the compromise of their sensitive PII or the need for them to take protective steps, to the extent possible.

> **October 25, 2023 Update**
>
> We anticipate restoring employee access to the Google Workspace for off-site users beginning Wednesday, October 25, 2023, at 5:00 p.m. Users may experience delays as they attempt to access Google Workspace outside of regular instructional and office hours. We expect fully restored access to be available by Thursday, October 26, 2023.
>
> Thank you for your understanding and commitment in creating a stronger security posture for CCSD.

38. On October 25, 2023, it was reported that some parents received an email that day titled "CCSD leak," informing them that their children's information had been compromised, and including PDF files with their children's pictures, contact information, student ID numbers, parent information and addresses.[6] Certain parents were reported by Channel 3 News to have received the "CCSD leak" email and attachments. [7]

39. The sender's name is listed as "Cadence Martin," and the email appeared to originate from an email address connected to with the Coalinga-Huron Unified School District in California. Coalinga-Huron Unified School District confirmed that one of their student account's

[6] https://news3lv.com/news/local/some-ccsd-families-worried-after-receiving-email-from-california-school-district-with-pictures-private-info-about-their-children (last visited October 31, 2023).

[7] *Id.*

was breached and used to send the emails to CCSD parents.[8]

40. The email states:

> I'm so sorry to tell you this but unfortunately your private information has been leaked. You should probably change your information in CCSD systems if that is possible.
>
> There are over 200,000 student profiles like this which have been leaked now by the hackers.
>
> Be careful out there. Don't shoot the messenger! [9]

41. Expressing that the received email was "scary," a parent who received the email was quoted as stating, "I do think that CCSD needs to tell us what's going on because we're not getting answers. We're all left in the dark."[10]

42. On that same day, according to an article posted by DataBreaches.net, SingularityMD posted a statement and links to even more leaked CCSD files. The statement was also emailed directly to parents of children enrolled at CCSD. The statement said, in part:

> We SingularityMD (the hack team), would like to make a statement for clarification. CCSD did not detect a security issue, we emailed them to tell them we had been in their network for a few months.
>
> For 6 years they forced students to use their birthday as their password, resetting the passwords back to their birth date each year, they even prevented the students from securing their accounts.
>
> . . .
>
> We asked for less than one third of the Jesus F Jara's annual salary in exchange for destroying the stolen data.
>
> The callousness and incompetence of the leadership at CCSD is astounding, not only did they not cooperate, it is clear they did not communicate with principals and have still not plugged their leaky ship, meaning we still have access to the network.
>
> . . .

---

[8] *See* https://www.govtech.com/education/k-12/parents-get-worrying-emails-after-clark-county-wash-cyber-incident (last visited October 31, 2023).

[9] *Id.*

[10] *Id.*

> As promised to them in our initial correspondence we are now leaking the 200k student profiles we extracted from their network yesterday, these profiles include a photo, birth date, person ID, student Number, State Student ID, Email, Language, Race / Ethnicity, Household names, relationships, and contact information, outside household contact information.
>
> One final tip for CCSD, we will continue to cause trouble until you pay, or you finally kick us out of your network.

The statement reportedly included more leaked files along with evidence that the ransomware group still had access to the District's email server.[11]

43. Also that evening, CCSD sent an email to its employees outlining new Google Workspace controls that the District will be implementing "in an effort to safeguard our data and communication," including multi-factor authentication ("MFA") for shared and generic accounts. However, the District said that MFA would not be required for student accounts. In addition, employees would be prohibited from automatically forwarding their emails, and document sharing outside of CCSD for some students would be restricted.[12]

/ / /

/ / /

/ / /

[11] https://www.databreaches.net/hackers-escalate-leak-200k-ccsd-students-data-claim-to-still-have-access-to-ccsd-email-system/ (last visited October 31, 2023).

[12] *See*, https://www.govtech.com/education/k-12/parents-get-worrying-emails-after-clark-county-wash-cyber-incident (last visited October 31, 2023).

44. On October 26, 2023, DataBreaches.net reported that some of the data exfiltrated from CCSD was released and available for download that week on a public file-sharing site. According to DataBreaches.net, the post accompanying these links included the following:[13]

- **25k Graduates with Personal Email, Birthdate, Ethnicity, PSAT scores.**
- **Diabetes Database MASTER 23_24** (Personal information on 1k students with diabetes)
- **Admin.zip** (Misc older spreadsheets 2016-2020. 45 MB)
- **HCM** (Financial reports, staff salaries, grant information 2019)
- **[0277] T3 ONLY.zip** (Incident reports for 2022 and 2023 by victim)
- **Swainston M.S. Attendance, Absent notes, Suspensions, Behavior referral tracking, student signout, bulling contracts, Truancy, Dress code violations, Early release, safety search, EMI – ASA, School Bus Incident Reports, Police Reports** (2 Files, 2.5 GB in total)
- **Internal Communications:**
  - **ZZZ-AIA-completed** (185 MB)
  - **GDA Grant Administrators** (1.3 GB)
  - **0003-ogc.RecordsRequest** (415 MB)
  - **CCSD Facilities Floor, Site and Portable Classrooms Plans** (409 MB)
  - **5 0449-VTCTA-Office Staff**
  - **Student – Census Verification Report – 12 Grade and Graduate photo and PII.** (800+ students. 78 MB)
- **HMS Super Users**
- **SPED Special Education levels per school.** (Student health conditions listed per School in the district. 38 MB)

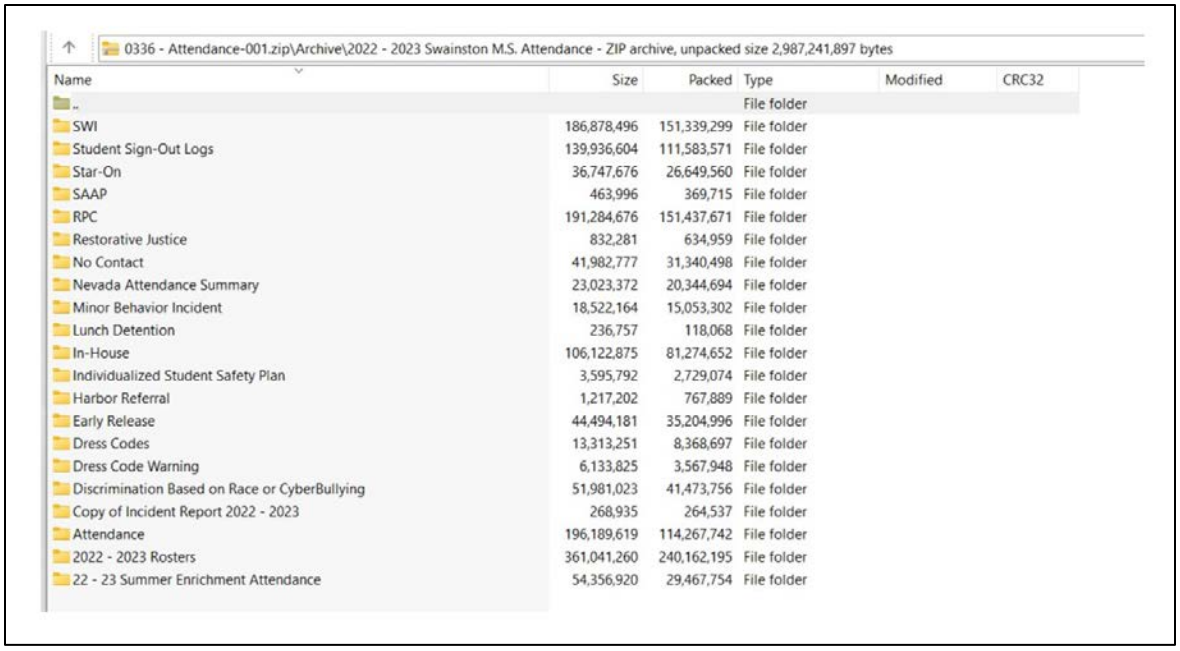
45. DataBreaches.net further reported that upon expanding certain folders, subfolders appeared that included "behavioral incident reports for named students, reports on named students who got lunch detention, and 251 reports on named students who got in-house school suspension. Other files contained the names of alleged bullying offenders and bullying victims with incident reports."

/ / /

/ / /

/ / /

[13] https://www.databreaches.net/exclusive-clark-county-school-district-student-data-begins-to-leak-ccsd-doesnt-comment/ (last visited October 31, 2023).



0336 - Attendance-001.zip\Archive\2022 - 2023 Swainston M.S. Attendance - ZIP archive, unpacked size 2,987,241,897 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
SWI	186,878,496	151,339,299	File folder		
Student Sign-Out Logs	139,936,604	111,583,571	File folder		
Star-On	36,747,676	26,649,560	File folder		
SAAP	463,996	369,715	File folder		
RPC	191,284,676	151,437,671	File folder		
Restorative Justice	832,281	634,959	File folder		
No Contact	41,982,777	31,340,498	File folder		
Nevada Attendance Summary	23,023,372	20,344,694	File folder		
Minor Behavior Incident	18,522,164	15,053,302	File folder		
Lunch Detention	236,757	118,068	File folder		
In-House	106,122,875	81,274,652	File folder		
Individualized Student Safety Plan	3,595,792	2,729,074	File folder		
Harbor Referral	1,217,202	767,889	File folder		
Early Release	44,494,181	35,204,996	File folder		
Dress Codes	13,313,251	8,368,697	File folder		
Dress Code Warning	6,133,825	3,567,948	File folder		
Discrimination Based on Race or CyberBullying	51,981,023	41,473,756	File folder		
Copy of Incident Report 2022 - 2023	268,935	264,537	File folder		
Attendance	196,189,619	114,267,742	File folder		
2022 - 2023 Rosters	361,041,260	240,162,195	File folder		
22 - 23 Summer Enrichment Attendance	54,356,920	29,467,754	File folder		

46. DataBreaches.net also confirmed that the leaked data contained personally identifiable medical information of students.[14]

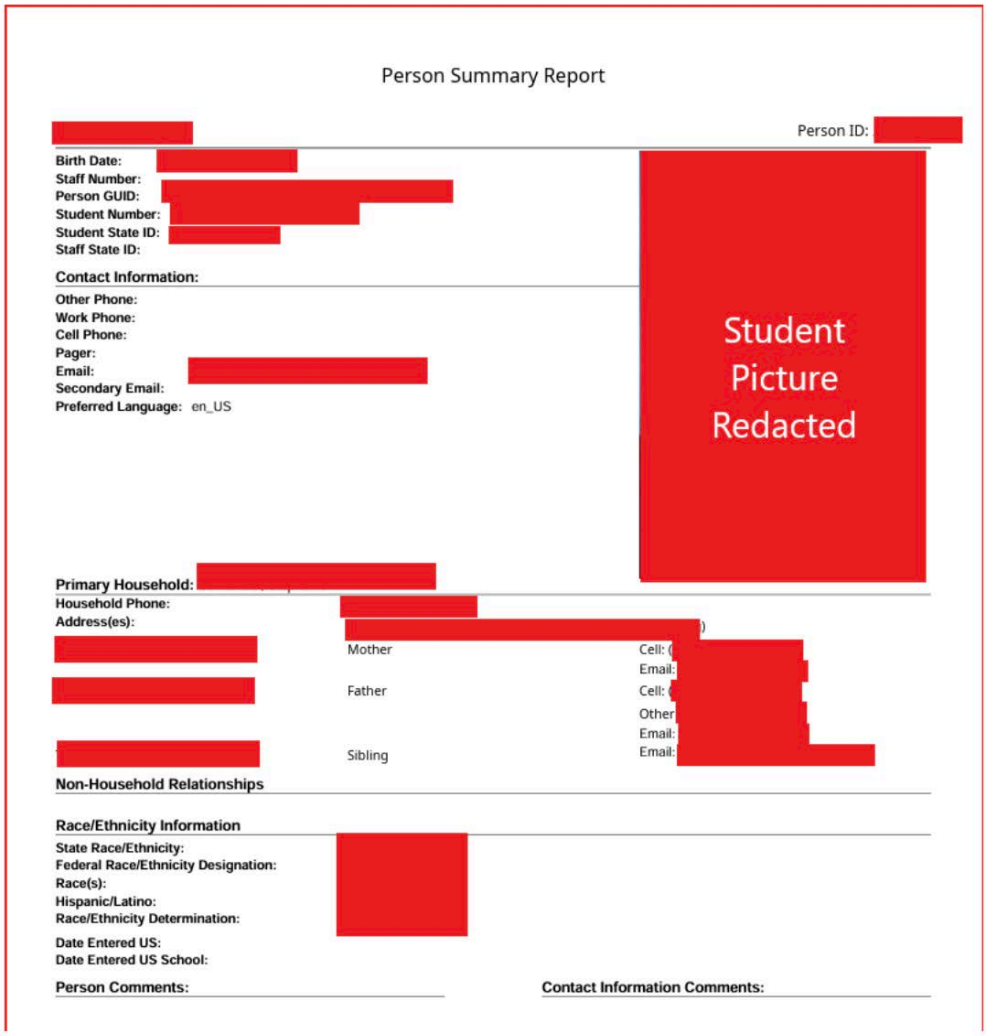
47. Email correspondence with the ransomware group caused DataBreaches.net to conclude that, at least as of late October 2023, SingularityMD still had access to CCSD's network.[15]

48. On October 27, 2023, DataBreaches.net reported that the ransomware group had leaked more highly sensitive files containing PII, including a "Master Register" with a list of over 300,000 students names, birthdates, and grades. This leak included over 14,000 pdf files and data, including students' names, student IDs, dates of birth, student email addresses, pictures, and household members' information including parents' and siblings names, cell phone numbers, email addresses, and other contact information. Race and ethnicity information is also included.[16] Redacted samples are below:

[14] *Id.*

[15] https://www.databreaches.net/hackers-escalate-leak-200k-ccsd-students-data-claim-to-still-have-access-to-ccsd-email-system/ (last visited October 31, 2023).

[16] *Id.*



Person Summary Report

[redacted] Person ID: [redacted]

Birth Date: [redacted]
Staff Number:
Person GUID: [redacted]
Student Number: [redacted]
Student State ID: [redacted]
Staff State ID:

Contact Information:

Other Phone:
Work Phone:
Cell Phone:
Pager:
Email: [redacted]
Secondary Email:
Preferred Language: en_US

Student Picture Redacted

Primary Household: [redacted]
Household Phone: [redacted]
Address(es): [redacted]

[redacted] Mother Cell: [redacted]
Email: [redacted]
[redacted] Father Cell: [redacted]
Other [redacted]
Email: [redacted]
[redacted] Sibling Email: [redacted]

Non-Household Relationships

Race/Ethnicity Information

State Race/Ethnicity: [redacted]
Federal Race/Ethnicity Designation:
Race(s):
Hispanic/Latino:
Race/Ethnicity Determination:

Date Entered US:
Date Entered US School:

Person Comments:

Contact Information Comments:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
1	Last Name	First Name	ID	DOB	G	School	Ind.	Type	MD	Order Date	Director	State	Signature	DIY AID			Plan of Ca
2	[redacted]				12					8/10/23	Stratford						
3					5					8/21/23	Forsberg		8/22/23				
4					8					2/22/23	Forsberg		8/9/23				
5					12					8/17/23	Strasser		8/17/23				
6					4					8/31/23	Enriquez						
7					8					8/4/23	Rodriguez		8/16/22				
8					12					8/3/23	Fossile		8/12/19				
9					11					02/2023	Kalekas		2/24/23				
10					11					7/24/23	Fossile		8/7/23				
11					2					4/7/23	Fossile		8/14/23				
12					9					8/15/23	Forsberg		8/16/23				
13					6					5/9/23	Kalekas		1/30/23				
14					8					8/23/23	Fossile		9/24/19				
15					5					7/10/23	Stratford		8/4/23				
16					9					10/16/22	Rodriguez		10/17/22				
17					9					8/4/23	Forsberg		8/4/23				
18					11					3/30/23	Fossile						
19					3					5/15/23	Forsberg		8/4/23				
20					12					9/26/23	Enriquez		12/3/19				
21					10					7/24/23	Stratford		8/9/23				
22					3					7/26/23	Rodriguez		8/4/23				
23					9					8/10/23	Strasser		8/14/23				
24					4					9/11/23	Kalekas		9/20/23				
25					10					7/26/23	Rodriguez		8/11/23				
26					5					8/15/23	Rodriguez		9/7/21				
27					2					8/17/23	Stratford		8/28/23				
28					3					6/1/23	Rodriguez		8/4/23				

Diabetes Mellitus tab from .csv file leaked. Image redaction by DataBreaches.net.

49. On October 31, 2023, DataBreaches.net reported that it established contact with SingularityMD, publishing the following, in part:

> DB: Did CCSD respond to you at all or have they just ignored all contacts from you?
>
> *SM: We had a dialog with them where they were provided proof of life (a 1GB sample of the data). The day of the deadline they asked for an extension to attempt to run our request past the board but then did not reply from that point onwards. There were approx 12 emails back and forth.*
>
> DB: If you're willing to say, how did you gain access to their network?
>
> *SM: We compromised a student account, then accessed information available to any student to escalate from there to teacher to systems level access for one or two systems. This was not a fancy high tech operation.*
>
> When DataBreaches asked how they were able to access the student's account, they responded that they obtained the student's date of birth (YYYYMMDD) from social media, and the email address from the student's account on "TikTok, etc." where the student ID had been used as the username because the student authenticated their school account when setting up the social media account. Asked to explain what information was available to any student that allowed them to escalate from the student's account to teacher to systems level, they replied:
>
> *SM: Google groups and google drives, if not configured correctly will expose teachers and staff files and conversations. In rare instances teachers have created shared drives and given the google group access to this drive. So if one was to add themselves to the group, they can then also access the drive contents. Nothing fancy at all.*

50. Despite these continuing alarming revelations about the scope and sensitivity of the data accessed and published by these cyber-attackers, CCSD has refused to notify its staff and student community about the true nature of this ransomware attack, keeping many affected individuals in the dark, unaware that some of their most sensitive information has been publicly disclosed and that they should, at a bare minimum, take steps to protect themselves against identity theft.

B. Defendants Have a Duty to Protect the Electronic PII They Store under State and Federal Law.

51. According to the District, CCSD oversees and manages medical conditions of all students, provides and implements specialized health care procedures, and develops and maintains

procedures for medication administration. School psychologists for the District deliver school-based psycho-educational services intended to improve students' academic performance and behavior, enhance their overall educational success, and promote mental health. In addition, School Health Services are provided by CCSD. Services are provided in the school setting and may include but are not limited to: behavior/mental health services, nursing services, physical therapy, occupational therapy, speech therapy, and audiological services.

52. Based at a minimum on such significant health-related activities, Defendants are entities either directly or indirectly covered by HIPAA, they must comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C, which establish national security standards and duties for Defendants' protection of PII maintained by them in electronic form.

53. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

54. "Electronic protected health information" (hereinafter, "PHI") is defined as "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

55. HIPAA's Security Rule requires Defendants to (a) ensure the confidentiality, integrity, and availability of all electronically protected health information the covered entity or business associate creates, receives, maintains, or transmits; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (c) protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and (d) ensure compliance by their workforce.

56. HIPAA also requires Defendants to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(c), and to "[i]mplement technical

policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

57. The cyberattack on Defendants, particularly given the available information provided to them months before the attack, establishes they did not follow these Rules. This attack resulted directly from insufficiencies that show Defendants violated safeguards mandated by HIPAA regulations, including, but not limited to:

(a) Failing to ensure the confidentiality and integrity of electronic PHI that Defendants create, receive, maintain, and transmit, in violation of 45 C.F.R. section 164.306(a)(1);

(b) Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those people or software programs granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);

(c) Failing to put policies and procedures into practice to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. section 164.308(a)(1);

(d) Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);

(e) Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. section 164.306(a)(2);

(f) Failing to protect against any reasonably expected uses or disclosures of electronic PHI not permitted under the privacy rules about individually identifiable health information, in violation of 45 C.F.R. section 164.306(a)(3);

(g) Failing to ensure compliance with HIPAA security standard rules by its workforce, in violation of 45 C.F.R. section 164.306(a)(4);

(h) Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized people, in violation of 45 C.F.R. section 164.502, *et seq.*;

(i) Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures for PHI as necessary and appropriate for

the members of its workforce to carry out their functions and to maintain the security of PHI, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and

(j) Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. section 164.530(c).

58. Defendants also violated the duties applicable to them under the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq*. ("FTC Act"), from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that an entity's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.[17]

59. Additionally, Defendants violated the Family Educational Rights and Privacy Act ("FERPA"). FERPA requires that an education institution must have a policy or practice of prohibiting the release of education records or providing access to any personally identifiable information in education records, unless there is prior written consent of a parent or eligible student, except as authorized by law. *See* 20 U.S.C. § 1232g(b)(1)–(2). Similarly, 34 C.F.R. § 99.30 provides that a "parent or eligible student shall provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from the student's education records, except as provided in § 99.31." To "Disclose" is defined as "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 C.F.R. § 99.3.

60. Moreover, Defendants violated additional mandatory duties imposed by Nevada state statutes, regulations, and their own mandated policies enacted to protect the confidentiality, security and integrity of employee and student records, and to protect against violations of employee and student privacy, breach and exposure of employee and student confidential information, and the risk of identity theft. These enactments include, but are not limited to:

[17] *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

- NRS 603A.210 (requiring that data collectors maintain reasonable security measures to protect personal information);
- NRS 603A.220 (requiring that data collectors provide timely notice of data breaches);
- NRS 392.029 (requiring public schools to protect education records from release without written consent);
- NAC 388.289 (requiring that confidentiality of personally identifiable information of special education students be protected at its collection, storage, disclosure, and destruction);
- Clark County School District Policy 5125 (recognizing the confidential nature of student records);
- CCSD Regulation 5125.1 (recognizing that all school records of students are "confidential" and may only be released to particular individuals upon written request);
- CCSD Policy 5138 (requiring that the District protect the privacy of students with diverse gender identities or expressions, and prohibiting it from disclosing information that may reveal a student's gender identity or expression status);
- CCSD Regulation 4311 (providing that personnel information regarding District employees is confidential and may only be reviewed on a need-to-know basis); and
- CCSD Regulation 1212 (promising that confidential information concerning all personnel will be safeguarded by the District);

61. The enactments set forth above, and each of them, imposed on CCSD mandatory duties to protect the data at issue from cyberattacks, which they failed to uphold.

62. The enactments violated by Defendants enumerated herein were designed to protect against the particular kind of injury suffered by Plaintiffs and Class members, such as identity theft or the risk of identity theft, identity theft or the risk of identity theft from misuse of Social Security numbers, disclosure of confidential student and employee information, intentional interference with Plaintiffs' and Class members' interest in solitude, seclusion or preventing the public disclosure of private facts, either as to their persons or as to their private affairs or concerns and

those of their families, of a kind that would be highly offensive to a reasonable person; loss of time and money to monitor their finances for fraud, and loss of control over their PII; failing to protect and preserve confidentiality of PII of Plaintiffs and Class members against disclosure and release, invasion of privacy, breach of the confidentiality of their PII and costs and time associated with remedying such breaches, the financial and temporal cost of monitoring their credit reports and financial accounts, time expended in addressing the outfall from this attack, and/or increased risk of future harm.

63. Defendants' failure to perform their mandatory duties under the enactments enumerated herein were a substantial factor in causing, and/or proximately caused, Plaintiffs' and Class members' harms as set forth herein.

64. As established by these laws, Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, keeping, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

65. Defendants also owed a duty to Plaintiffs and Class members to provide reasonable security in compliance with industry standards and state and federal requirements and to ensure that their computer systems, networks, and protocols adequately protected this PII and were not exposed to infiltration. This included a duty to Plaintiffs and Class members to, *inter alia*: (a) design, maintain, and test their computer systems to ensure that the PII in their possession was adequately secured and protected; (b) create and implement reasonable data security practices and procedures to safeguard the PII in their possession; (c) avoid unauthorized access to their computer systems through common attacks such as phishing; (d) adequately train employees and others who accessed information within their systems on how to adequately protect PII; (e) avoid permitting this type of infiltration such as by use of multi-factor authentication and reasonable password hygiene; (f) implement processes and procedures that would detect a breach of their data security systems promptly and to act on data security warnings and alerts promptly; (g) disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft or exfiltration; and (h) disclose in a timely and correct manner when data breaches,

ransomware leaks, or cyberattacks occurred. Defendants owed these duties to Plaintiffs and Class members because they were foreseeable and probable victims of CCSD's inadequate data security practices.

66. Defendants affirmatively designed their systems with insufficient user authentication, security protocols, and privileges and set up faulty patching and updating protocols and backup systems. These affirmative decisions resulted in unauthorized third parties executing the cyberattack at issue and exfiltrating this data, to the injury and detriment of Plaintiffs and Class members. By taking affirmative acts inconsistent with these obligations that left CCSD's computer systems vulnerable to attack, Defendants revealed and permitted the disclosure of PII to unauthorized third parties. Through such actions or inactions, CCSD failed to preserve the confidentiality of PII they were duty-bound to protect.

67. As a direct and proximate result of Defendants' actions, inactions, omissions, breaches of and failures to perform their duties and want of ordinary care that directly and proximately caused or resulted in the cyberattack and the resulting data breach, Plaintiffs and Class members have suffered and will continue to suffer damages and other injury and harm in the form of, *inter alia*: (a) present, imminent, immediate, and continuing increased risk of identity theft, identity fraud, and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation for the time, effort, and funds they must expend; (b) invasion of privacy; (c) breach of the confidentiality of their PII and costs and time associated with remedying such breaches; (d) deprivation of the value of their PII, for which there is a well-established national and international market, (e) refusal to pay statutory damages to which they are entitled even without proof of access or actual damages; (f) lost computer and phone storage space as a result of unwanted spam, emails or unsolicited telephone calls; (g) the financial and temporal cost of monitoring their credit reports and financial accounts; (h) time expended in addressing the fallout from this attack; and/or (i) increased risk of future harm.

/ / /

/ / /

/ / /

C. The Value of PII Shows Plaintiffs and the Class Were Injured as a Result of this Unauthorized Access.

68. It is well known that PII is a valuable commodity[18] and the frequent target of hackers, such that Plaintiffs and Class members would lose value if their data was permitted to be improperly accessed or stolen.

69. Defendants either were or should have been aware that the PII they collected is highly sensitive and of significant value to those who would use it for wrongful purposes. As the FTC has reported, identity thieves can use this information to commit an array of crimes, including identity theft and medical and financial fraud.[19]

70. A robust cyber black market exists where criminals post stolen PII on multiple underground Internet websites, commonly called the dark web, to create fake insurance claims, buy and resell medical equipment, or access prescriptions for illegal use or resale. Criminals often trade stolen PII on the "cyber black market" for years following a breach. For example, it is believed that identity thieves used certain PII compromised in the 2017 Experian data breach three years later to apply for COVID-19-related benefits.[20] According to a 2017 Javelin strategy and research presentation, fraudulent activities based on information stolen in data breaches between two and six years old had increased by nearly 400% over the previous four years.[21] Thus, offering only a year of credit monitoring is facially inadequate.

---

[18] *See*, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (*citations omitted*).

[19] Federal Trade Commission, What to Know About Identity Theft, https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited 5/3/22).

[20] Janelle Stecklein, *Director: 64,000-plus fraudulent unemployment claims 'mitigated'*, The Duncan Banner (June 24, 2020), https://www.duncanbanner.com/news/director-64-000-plus-fraudulent-unemployment-claims-mitigated/article_dc446671-73a6-5e8a-b732-bcedba72b458.html (last visited 5/3/22).

[21] *See*, Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web* (2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited 5/3/22).

71. According to Experian, one of the three major credit bureaus, medical records can be worth up to $1,000 per person on the dark web, depending on completeness.[22] PII and PHI can be sold at a price ranging from around $20 to $300.[23]

72. The Ponemon Institute found that medical identity theft can cost victims an average of $13,500 per incident and that victims must often pay off the imposter's medical bills to resolve the breach.[24]

73. In another study by the Ponemon Institute in 2015, 31% of medical identity theft victims lost their healthcare coverage because of the incident, 29% had to pay to restore their health coverage, and over half could not resolve the identity theft.[25]

74. Once PII is stolen, particularly such as student or employee identification numbers or Social Security numbers, fraudulent use of that information and damage to victims may continue for years, as the fraudulent use of this data resulting from the attack may not come to light for years—demonstrating why one year of credit monitoring is inadequate. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches: "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[26]

---

[22] *Id.*

[23] https://www.privacyaffairs.com/dark-web-price-index-2021/ (last visited October 31, 2023).

[24] Brian O'Connor, Healthcare Data Breach: What to Know About Them and What to Do After One, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited 5/3/22).

[25] Ponemon Institute, *Fifth Annual Study on Medical Identity Theft*, (February, 2015), http://www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf (last visited 5/3/22).

[26] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm (last visited 5/3/22).

75. The ramifications of Defendants' failure to keep this PII secure from a cyberattack and then not timely advising affected persons of all the relevant facts are thus not temporary but long-lasting, as the fraudulent use of that information and damage to victims may continue for years. That is why providing prompt, accurate, and fulsome notice to consumers as expeditiously as possible is necessary so they can take action to protect themselves. Yet, Defendants are still refusing even to acknowledge the extent of the attack, whether it was a ransomware attack that took place, or provide timely, proper, and appropriately comprehensive notice in the most expedient time possible and without unreasonable delay, as required under Nevada law. Defendants have also failed and/or refused to even limit the potential extent of damage by ensuring that the hackers no longer have access to the District's computer systems.

76. Thus, as a direct and proximate result of Defendants' breaches of confidence, Plaintiffs and Class members have suffered and will continue to suffer injury and damages, including, *inter alia*: (a) actual identity theft or compromise; (b) the loss of the opportunity to control how their PII is used; (c) the compromise, publication, and theft of their PII; (d) time and expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and unauthorized use of their PII, such as set forth for Plaintiffs above; (e) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the cyberattack, including, but not limited to, time and effort spent researching how to prevent, detect, contest, and recover from fraud and identity theft and implementing measures to do so; (f) costs associated with placing freezes or monitoring on credit reports; (g) the continued risk to their PII, which remain in Defendants' possession, custody or control and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of current and former students and employees and all of their beneficiaries and dependents; (h) lost computer and phone storage space as a result of unwanted spam, emails or unsolicited telephone calls, and/or (i) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the attack.

/ / /

CLASS ALLEGATIONS

77. Plaintiffs, in their capacities stated above and on behalf of all others similarly situated, bring this action pursuant to Nevada Rule of Civil Procedure 23. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements for class certification.

78. The Class is defined as all Nevada citizens whose data was compromised and/or who received or will receive notice of this attack from CCSD, from October 2023 to the present (the "Class").

79. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether class certification is appropriate.

80. The members of the Class are sufficiently numerous such that the joinder of all Class members is impracticable. The proposed Class contains past or current CCSD employees and their dependents as well as students that, while not verified by CCSD, would be in the hundreds of thousands of persons who had unique records about them improperly accessed or taken.

81. Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual Class members. The factual basis underlying Defendants' misconduct is common to all Class members and represents a common thread of unlawful, reckless, negligent, or grossly negligence conduct, resulting in injury to all members of the Class. These common legal and factual questions include the following:

(a) Whether CCSD implemented and maintained reasonable security practices and procedures appropriate to protect Plaintiffs' and Class members' PII from unauthorized access, destruction, use, theft, modification, or disclosure;

(b) Whether Defendants and their contractors, subcontractors, employees, agents, officers, or directors negligently or otherwise unlawfully disclosed or permitted the unauthorized disclosure of Plaintiffs' and Class members' PII to unauthorized persons or provided negligent or reckless oversight of the actions of CCSD;

(c) Whether CCSD had taken adequate steps to ensure it had not negligently or recklessly created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs'

and Class members' PII and failed to protect and preserve the integrity of the PII found on CCSD's computer systems;

(d) Whether Defendants' actions or inactions were a proximate result of the negligent or reckless release of confidential information or records concerning Plaintiffs and Class members;

(e) Whether Defendants failed to ensure that CCSD adequately, promptly, timely, and accurately informed Plaintiffs and Class members that their PII had been compromised and whether Defendants violated the law by failing to promptly and fully notify Plaintiffs and the Class members of this material fact;

(f) Whether CCSD has adequately addressed and fixed the vulnerabilities that permitted the cyberattack and resulting data breach to occur;

(g) Whether Defendants violated provisions of NRS Chapter 603A – Security and Privacy of Personal Information and the other laws cited herein; and

(h) Whether Plaintiffs and the Class are entitled to damages, equitable and/or injunctive relief to redress the harm faced as a result of the cyberattack and Defendants' failure to provide full and adequate notice thereof, and the scope of such relief.

82. Plaintiffs' claims are typical of the claims of other Class members. There is no unique defense available to Defendants as Plaintiffs, like all Class members, were subject to the unauthorized disclosure of PII as a result of Defendants' conduct.

83. Plaintiffs will fairly and adequately represent the interests of Class members. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions, including data breaches concerning the sensitive PII of individuals. Plaintiffs and counsel are committed to vigorously prosecuting the action on behalf of the Class. Neither Plaintiffs nor counsel have any interest materially adverse to or that irreconcilably conflicts with those of other Class members.

84. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitive, may have no effective and complete remedy, and may not even learn of the true scope of the wrongful conduct at issue. Class treatment of common questions of law

and fact is also superior to multiple individual actions or piecemeal litigation and results in substantial benefits in that it conserves the resources of the courts and litigants and promotes consistency and efficiency of adjudication. The conduct of this action as a class action presents few management difficulties and protects the rights of each Class member. Plaintiffs thus anticipate no difficulty in the management of this case as a class action and providing notice to members of the Class.

85. Class treatment is also appropriate because Defendants have acted on grounds generally applicable to members of the Class, making class-wide equitable, injunctive, declaratory, and monetary relief appropriate.

86. Notice of the pendency or resolution of this action can be provided as Defendants have contact information for all or a significant majority of Class members.

FIRST CLAIM FOR RELIEF

Violation of NRS 41.600 - Actions by Victims of Fraud

87. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Claim for Relief and the relief available thereunder.

88. NRS 41.600(1) provides a private right of action to a person who is a victim of consumer fraud.

89. NRS 41.600(2)(e) defines consumer fraud as a deceptive trade practice as defined in NRS 598.0915 to 598.0925, inclusive.

90. NRS 603A.260 provides that a violation of the provisions of NRS 603A.010 to 603A.290, inclusive, constitutes a deceptive trade practice for the purposes of NRS 598.0903 to 598.0999, inclusive.

91. NRS 603A.040 defines "Personal information" as a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: (a) Social security number; (b) Driver's license number, driver authorization card number or identification card number; (c) Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account; (d) A medical

identification number or a health insurance identification number; or (e) A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account.

92. CCSD is a "data collector" within the meaning of NRS 603A.030 as it is a governmental agency that handles, collects, disseminates or otherwise deals with nonpublic personal information.

93. CCSD violated NRS 603A.210(1), which requires that a data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.

94. CCSD did not implement and maintain such reasonable security measures, as shown by the massive ransomware attack successfully implemented against it, wherein the District failed to protect the records of students, former students, and staff from unauthorized access, acquisition, use and disclosure, as detailed above.

95. CCSD also violated NRS 603A.210(2), which requires that if a data collector is a governmental agency and maintains records which contain personal information of a resident of this State, the data collector shall, to the extent practicable, with respect to the collection, dissemination and maintenance of those records, comply with the current version of the CIS Controls as published by the Center for Internet Security, Inc. or its successor organization, or corresponding standards adopted by the National Institute of Standards and Technology of the United States Department of Commerce.

96. CCSD failed to comply with the current version of CIS Controls or corresponding standards adopted by the National Institute of Standards and Technology. For example, the District failed to effectively develop processes and technical controls to identify, classify, securely handle, and retain data; encrypt sensitive data at rest; protect data at rest; use unique passwords of sufficient length and including multi-factor authentication for all enterprise assets, require all externally-exposed enterprise or third-party applications to enforce MFA, where supported; prevent or control the installation, spread, and execution of malicious applications, code, or scripts

on enterprise assets; authenticate users, devices and other assets commensurate with the risk of the transaction; implement protections against data leaks; detect malicious code; and monitor its network to detect potential cybersecurity events.

97. Further, as described in detail above, on or about October 5, 2023, CCSD suffered a breach of the security of its system data within the meaning of NRS 603A.020, which provides as follows: "'Breach of the security of the system data' means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the data collector."

98. NRS 603A.220 provides that any data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system data.

99. The notification required by NRS 603A.220 may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that the notification will not compromise the investigation.

100. A data collector must provide notification using at least one of the methods provided for by NRS 603A.220.

101. In violation of NRS 603A.220, CCSD failed to ensure that it gave prompt, timely, and fulsome notice of the attack and resulting data breach.

102. CCSD's violations of NRS 603A.210 & .220 constitute "consumer fraud" for purposes of NRS 41.600(2)(e).

103. As a direct and proximate result of Defendants' violations of NRS Chapter 603A, Plaintiffs and Class Members have been damaged in excess of $15,000, in an amount to be determined at trial.

104. Plaintiffs and Class Members are further entitled to damages according to proof, costs, and any equitable relief the Court deems appropriate under NRS 41.600(3)(b).

105. Plaintiffs and Class Members have been forced to retain the services of an attorney to prosecute this matter and are entitled to recover their reasonable costs and attorneys' fees pursuant to Nevada law, including, but not limited to, under NRS 41.600(3)(c).

SECOND CLAIM FOR RELIEF

Violation of the Nevada Deceptive Trade Practices Act, NRS 598.0901, *et seq*.

106. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Claim for Relief and the relief available thereunder.

107. NRS 603A.260 provides that a violation of the provisions of NRS 603A.010 to 603A.290, inclusive, constitutes a deceptive trade practice for the purposes of NRS 598.0903 to 598.0999, inclusive.

108. As described above, CCSD violated NRS 603A.210 and 603A.220. These violations therefore constitute deceptive trade practices for the purposes of NRS 598.0903 to 598.0999, inclusive.

109. Class members, including, but not limited to Plaintiff John Doe, that fall within the protected groups addressed in the above-referenced statutes have damages in excess of $15,000, as a direct and proximate result of these deceptive trade practices, in an amount to be determined at trial.

110. Such Class members have been forced to retain the services of an attorney to prosecute this matter and are entitled to recover their reasonable costs and attorneys' fees pursuant to Nevada law, including, but not limited to, under NRS 598.0977.

111. Such Class members also are entitled to recover punitive damages in accordance with Nevada law, including, but not limited to, NRS 598.0977, and the Court should also impose civil penalties on Defendants as permitted under NRS 598.0973(1) and 598.0975(1).

THIRD CLAIM FOR RELIEF

Negligence and Negligence Per Se

112. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth

herein to the extent relevant to this Claim for Relief and the relief available thereunder.

113. Defendants collected, came into possession of, and maintained Plaintiffs' and Class members' PII and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and disclosed to unauthorized parties.

114. Defendants had a special relationship with Plaintiffs and Class members who entrusted Defendants with adequately protecting their PII.

115. Defendants knew that the PII was private and confidential and must be protected as private and confidential. Thus, Defendants owed a duty of care not to subject Plaintiffs and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices. Defendants knew or should have known of the risks inherent in collecting and storing PII, the vulnerabilities of CCSD's data security systems, and the importance of adequate security. Defendants were required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class members' PII.

116. Defendants' actions or inactions described above violated the laws and regulations set forth above, including NRS 598.0903 *et seq.*, NRS 603A.210 & .220, NRS 392.029, and NAC 388.289. Defendants' actions and inactions described above also violated federal statutes and regulations, including the FTC Act, FERPA, HIPAA, the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E, and HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections identified above, as well as CCSD Policy Numbers 5125 & 5138 and CCSD Regulation Numbers 1212, 4311 and 5125.1.

117. Plaintiffs and Class members are within the class of persons that these statutes and rules were designed to protect. Defendants breached the duties established by those laws and rules by failing to ensure that CCSD would employ industry standard data and cybersecurity measures to ensure compliance with the subject laws, including, but not limited to, proper segregation, access controls, multi-factor authentication, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

118. Defendants' conduct in violation of these applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiffs' and Class members' PII and thus Plaintiffs and Class members have suffered and will continue to suffer damages as a result of Defendants' conduct.

119. It was reasonably foreseeable, particularly given the growing number of data breaches of information held by school districts, that the failure to reasonably protect and secure Plaintiffs' and Class members' PII in compliance with applicable laws would result in an unauthorized third party gaining access to CCSD's networks, databases, and computers that stored or contained Plaintiffs' and Class members' PII, resulting in Defendants' presumptive liability under principles of negligence *per se*.

120. Defendants knew, or should have known, of CCSD's heightened vulnerability to cyberattacks and breaches by cybercriminals. Based on the facts detailed above, including an attack on their own servers in 2020, Defendants knew or should have known about the threat posed to it. Defendants' failure to ensure that CCSD took proper security measures to protect Plaintiffs' and Class members' PII created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of PII by unauthorized third parties. As described above, given that school districts—including CCSD—were known at the time of the attack to be prime targets for hackers, Plaintiffs and Class members are part of a foreseeable, discernable group that was at high risk of having their PII compromised, exfiltrated, and otherwise wrongly disclosed, if not adequately protected by Defendants. It was also reasonably foreseeable that Plaintiffs and Class members would sustain injuries if CCSD failed to provide timely, direct, understandable, and complete notice of this data breach to Plaintiffs and Class members.

121. Defendants had a duty to ensure that CCSD employees would employ reasonable security measures, systems, processes, and otherwise protect the PII of Plaintiffs and Class members pursuant to the state and federal laws set forth above, resulting in Defendants' liability under principles of negligence.

122. Defendants had a duty to ensure that CCSD employees would employ reasonable security procedures, systems, and processes to detect cyberattacks and to timely act on warnings

about data breaches and other forms of cyberattacks.

123. Defendants owed a duty to ensure that CCSD would timely and adequately inform Plaintiffs and Class members, in the event of a data breach, that their PII had been compromised or improperly disclosed as part of a cyberattack to unauthorized third parties.

124. Defendants failed to ensure that CCSD would provide adequate security for data in their possession or over which they had supervision and control.

125. Defendants, through their actions and omissions, unlawfully breached their duties to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class members' PII within Defendants' possession, supervision, and control.

126. Defendants, through their actions and omissions, unlawfully breached duties owed to Plaintiffs and Class members by failing to ensure that CCSD would have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class members' PII.

127. Defendants, through their actions and omissions, unlawfully breached duties to ensure that CCSD would timely and fully disclose to Plaintiffs and Class members that their PII within Defendants' possession, supervision, and control was compromised, the nature of the compromise, and precisely the type of information compromised. Defendants' breach of duties owed to Plaintiffs and Class members proximately caused Plaintiffs' and Class members' PII to be compromised and for them to suffer losses, including direct economic losses for which they seek compensation in damages. Plaintiffs' and Class members' PII constitutes personal property that was stolen as a proximate result of Defendants' negligence, resulting in harm, injury, and damages to Plaintiffs and Class members.

128. As a result of Defendants' ongoing failure to adequately notify Plaintiffs and Class members regarding what type of PII has been compromised, Plaintiffs and Class members are unable to take the necessary precautions to mitigate damages by preventing future fraud for which they seek compensation in damages.

129. Defendants' breaches of duty caused Plaintiffs and Class members to suffer from increased risk of identity theft, loss of time, property and money, and loss of control over their PII.

130. As a proximate result of Defendants' negligence and breach of duties, Plaintiffs and Class members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

131. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order compelling Defendants to institute appropriate data collection and safeguarding methods and policies with regard to PII and provide full and complete notice to all affected persons, as set forth below.

FOURTH CLAIM FOR RELIEF

Breach of Confidence

132. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Claim for Relief and the relief available thereunder.

133. At all times during Plaintiffs' and Class members' interactions with CCSD, Defendants were required to ensure that it was aware of the confidential and sensitive nature of Plaintiffs' and the Class members' PII that Plaintiffs and Class members provided to Defendants.

134. As alleged herein, Defendants' relationship with Plaintiffs and Class members was governed by the reasonable expectations that Plaintiffs' and the Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

135. Plaintiffs and Class members provided their PII with the explicit and implicit understandings that it would be protected, and that such PII would not be permitted to be disseminated to any unauthorized third parties, and that the persons who had access to such data would take precautions to protect that PII from unauthorized disclosure.

136. Defendants voluntarily received, in confidence, Plaintiffs' and Class members' PII with the understanding that such information would not be disclosed or disseminated to the public or any unauthorized third parties.

137. As a proximate result of Defendants' failure to prevent and avoid the attack and resulting data breach at issue here, Plaintiffs' and Class members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and the Class members'

confidence, and without their express permission.

138. But for Defendants' disclosure of Plaintiffs' and the Class members' PII in violation of the parties' understanding and reasonable expectation of confidence, Plaintiffs' and Class members' PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Such actions and inactions by Defendants were the direct, proximate, and legal cause of the exfiltration of Plaintiffs' and Class members' PII as well as the resulting damages.

139. The injury and harm Plaintiffs and the Class members suffered was the reasonably foreseeable result of Defendants' conduct, which permitted the unauthorized disclosure of Plaintiffs' and Class members' PII.

140. Defendants either knew, or should have known, that CCSD's methods of accepting and securing Plaintiffs' and the Class members' PII was inadequate as it relates to securing servers and other computer equipment containing Plaintiffs' and Class members' PII.

141. As a direct and proximate result of Defendants' actions and omissions as detailed above that resulted in breaches of confidence to Plaintiffs and Class members, Plaintiffs and Class members have suffered and will suffer injury, harm and damages as set forth in detail above.

142. Plaintiffs thus seek injunctive relief on behalf of the Class in the form of an order compelling Defendants to institute appropriate data collection and safeguarding methods and policies with regard to PII, as set forth below.

FIFTH CLAIM FOR RELIEF

Breach of Fiduciary Duty

143. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Claim for Relief and the relief available thereunder.

144. Plaintiffs and Class members gave Defendants their PII in confidence, reasonably believing that Defendants would protect that information. Plaintiffs and Class members would not have provided Defendants with this information had they known it would not be adequately protected.

145. Defendants' acceptance and storage of Plaintiffs' and Class members' PII, as well

as for Plaintiffs and many members of the Class, their status as employees and students of CCSD, created a fiduciary relationship between Defendants, on the one hand, and Plaintiffs and Class members on the other hand. In light of this relationship, Defendants must act primarily for the benefit of such persons, which includes safeguarding and protecting Plaintiffs' and Class members' PII.

146. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship. CCSD breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class members' PII, failing to comply with the data security guidelines set forth in the state and federal laws and regulations set forth above, and otherwise failing to safeguard Plaintiffs' and Class members' PII that it collected.

147. As a direct and proximate result of Defendants' breaches of fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury as set forth in detail above.

148. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order compelling Defendants to institute appropriate data collection and safeguarding methods and policies with regard to PII, as set forth below.

SIXTH CLAIM FOR RELIEF

Breach of Implied Contract

149. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Claim for Relief and the relief available thereunder.

150. Plaintiffs and Class Members were required to provide their PII, including their names, addresses, dates of birth, telephone numbers, email addresses, various forms of identification, medical information, and other sensitive private PII to Defendants, or allow it to be stored with Defendants, as a condition of their employment, attendance at CCSD, or attendance of their dependents at CCSD.

151. Plaintiffs and Class Members provided their PII to Defendants in exchange for employment or the provision of educational or medical services, along with Defendants' promise to protect their PII from unauthorized disclosure.

152. In their written policies, CCSD expressly promised Plaintiffs and Class Members that they would only disclose PII under certain circumstances, none of which relate to the data breach at issue herein.

153. CCSD promised to comply with industry standards and applicable laws, like HIPAA, FERPA and the Individuals with Disabilities Education Act and to make sure that Plaintiffs' and Class Members' PII would remain protected.

154. Implicit in the agreement between Plaintiffs and Class Members and the Defendants to provide protected health information and other PII, was the latter's obligation to: (a) take reasonable steps to safeguard that PII, (b) prevent unauthorized disclosures of the PII, (c) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (d) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or use, and (e) retain the PII only under conditions that kept such information secure and confidential.

155. Without such implied contracts, Plaintiffs and Class Members would not have provided their PII to Defendants.

156. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendants, however, Defendants did not.

157. Defendants breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII, which was compromised as a result of the data breach at issue herein.

158. As a direct and proximate result of Defendants' breach of the implied contract between the parties, Plaintiffs and Class members have been damaged in excess of $15,000, in an amount to be determined at trial, and seek damages and are further entitled to injunctive relief in connection with the subject implied contract.

SEVENTH CLAIM FOR RELIEF

Unjust Enrichment

159. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Claim for Relief and the relief available thereunder. This claim

is pled in the alternative to other claims for relief set forth herein.

160. Defendants benefited from either directly or indirectly receiving Plaintiffs' and Class members' PII by their ability to retain and use that information for their own benefit. Defendants understood this benefit.

161. Defendants also understood and appreciated that Plaintiffs' and Class members' PII was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that information.

162. Defendants failed to ensure that CCSD would expend the resources necessary to provide reasonable security, safeguards, and protections to the PII of Plaintiffs and Class members, and saved millions of dollars as a result of their failure to invest in the appropriate infrastructure to protect such data. CCSD is liable to all persons impacted by this breach for the damage caused by this data breach incident and for unjust enrichment from the money they saved by not having adequate security systems in place.

163. Under principles of equity and good conscience, Defendants should not be permitted to retain money that should have been expended on such systems and from failing to implement appropriate data management and security measures mandated by industry standards.

164. Defendants wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class members.

165. Defendants' enrichment at the expense of Plaintiffs and Class members is and was unjust.

166. As a result of Defendants' wrongful conduct, as alleged above, Plaintiffs and Class members are entitled to equitable and injunctive relief.

EIGHTH CLAIM FOR RELIEF

Declaratory Relief

167. Plaintiffs incorporate the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Claim for Relief and the relief available thereunder.

168. A present and actual controversy exists between the parties.

169. Plaintiffs and Class members have a protectable interest in the controversies

between the parties.

170. Defendants have failed to acknowledge the wrongful nature of their actions, have not sent affected Plaintiffs and Class members adequate data breach notices regarding the attack and data theft at issue herein, nor publicly issued comprehensive corrective notices. Based on their inadequate disclosures to date, there is also no reason to believe that Defendants have taken adequate measures to ensure that CCSD would correct or enact adequate privacy policies and procedures to adequately protect and preserve Plaintiffs' and Class members' PII in Defendants' possession and control.

171. Now that Defendants' insufficient information security is known to hackers, the PII in Defendants' possession and control is even more vulnerable to cyberattack and is not less but more likely to take place.

172. Plaintiffs and Class members have no other adequate remedy of law in that, absent declaratory relief from the Court, Defendants are likely to not fully remedy the underlying wrong.

173. As described above, Defendants' actions have caused harm to Plaintiffs and Class members. Further, Plaintiffs and Class members are at risk of additional or further harm due to the exposure of their PII and Defendants' failure to fully address the security failings that led to such exposure and provide adequate notice thereof. Accordingly, the controversies between the Plaintiffs and Class members, on the one hand, and Defendants, on the other hand, are ripe for judicial determination.

174. Plaintiffs and Class members seek an order of this Court for declaratory, equitable, and injunctive relief in the form of an order finding that Defendants have failed and continue to fail to adequately protect Plaintiffs' and the Class members' PII from release to unknown and unauthorized third parties, requiring Defendants to correct or provide adequate privacy notices regarding this ransomware attack and data breach, implement security measures to protect and preserve Plaintiffs' and Class members' PII in Defendants' possession and control, and requiring Defendants to publicly issue comprehensive corrective notices to Plaintiffs, Class members and the public.

/ / /

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, in their stated capacities and on behalf of the Class and for the benefit of the public, pray for orders and judgments in favor of Plaintiffs and the Class and against Defendants as follows, as may be applicable to the Claims for Relief set forth above:

A. Finding that this action satisfies the prerequisites for maintenance as a class action under Nevada Rule of Civil Procedure 23 and certifying the Class defined herein;

B. Designating Plaintiffs as representatives of the Class and their counsel as Class counsel;

C. Declaring Defendants' conduct in violation of the laws set forth above, including, but not limited to, NRS 598.0903 *et seq.*, NRS 603A.210 & .220, NRS 392.029, NAC 388.289, the FTC Act, FERPA, HIPAA, the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C, and the other sections identified above.

D. An order:

1. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
2. prohibiting Defendants from refusing to promptly identify and send all affected persons adequately comprehensive data breach notices regarding the attack and data theft at issue herein in the form required by law;
3. prohibiting Defendants from failing to protect, including through encryption, all data collected through the course of their business operations in accordance with all applicable regulations, industry standards, and federal and state laws;
4. prohibiting Defendants from refusing to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and the Class members;
5. prohibiting Defendants from refusing to engage independent third-party security auditors/penetration testers as well as internal security personnel to

run automated security monitoring, database scanning and security checks and conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

6. prohibiting Defendants from refusing to audit, test, and train security personnel regarding any new or modified procedures;

7. prohibiting Defendants from refusing to ensure that CCSD will segment data by, *inter alia*, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

8. prohibiting Defendants from refusing 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 the employees' respective responsibilities with handling personal identifying information, as well as protecting the PII of Plaintiffs and Class members and preventing infiltration of Defendants' computer system by phishing processes by using such steps such as multi-factor authentication;

9. prohibiting Defendants from refusing to routinely and continually conduct internal training and education, and informing internal security personnel how to immediately identify and contain an attack or data breach when it occurs and what to do in response to a breach; and/or

10. prohibiting Defendants from refusing to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

E. All appropriate equitable relief;

F. Awarding Plaintiffs and Class members an award as compensation for damages as applies to the specific claims for relief identified above;

G. Awarding Plaintiffs' counsel reasonable attorneys' fees and non-taxable expenses;

H. Awarding Plaintiffs' costs;

I. Awarding pre- and post-judgment interest at the maximum rate permitted by applicable law; and

J. Granting such further relief as the Court deems just and proper.

Dated this 31st day of October, 2023.

SKLAR WILLIAMS PLLC

/s/ David B. Barney
Stephen R. Hackett, Esq., NSBN: 5010
Johnathon Fayeghi, Esq., NSBN: 12736
Matthew S. Fox, Esq., NSBN: 12884
David B. Barney, Esq., NSBN: 14681
410 South Rampart Blvd, Suite 350
Las Vegas, NV 89145
Telephone: (702) 360-6000
Facsimile: (702) 360-0000

WHATLEY KALLAS, LLP
Alan M. Mansfield, Esq.*
16870 W. Bernardo Drive, Suite 400
San Diego, CA 92127
Telephone: (619) 308-5034
Facsimile: (888) 341-5048

APRIL M. STRAUSS, A PC
April M. Strauss, Esq.*
2500 Hospital Drive, Bldg. 3
Mountain View, CA 94040
Telephone: (650) 281-7081

DOYLE APC
William J. Doyle, Esq.*
550 West B Street, 4th Floor
San Diego, CA 92101
Telephone: (619) 736-0000
Facsimile: (619) 736-1111

Attorneys for Plaintiffs and the Class

**Pro Hac Vice* application forthcoming.