WHATLEY KALLAS, LLP
Alan M. Mansfield, SBN: 125998
amansfield@whatleykallas.com
16870 W. Bernardo Drive, Suite 400
San Diego, CA 92127
Phone: (619) 308-5034
Fax: (888) 341-5048

APRIL M. STRAUSS, A PC
April M. Strauss, SBN: 163327
astrauss@sfaclp.com
2500 Hospital Drive, Bldg. 3
Mountain View, CA 94040
Phone: (650) 281-7081

DOYLE APC
William J. Doyle II, SBN: 188069
bill@doyleapc.com
Christopher W. Cantrell, SBN: 290874
chris@doyleapc.com
550 West B Street, 4th Floor
San Diego, CA 92101
Phone: (619) 736-0000
Fax: (619) 736-1111

Attorneys for Plaintiff

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SAN DIEGO

JANE ROE 1, on behalf of herself and all others similarly situated and for the benefit of the general public,

Plaintiff,

v.

SWEETWATER UNION HIGH SCHOOL DISTRICT and DOES 1 through 25, inclusive,

Defendants.

Case No. 37-2023-00028588-CU-BT-CTL

CLASS ACTION COMPLAINT FOR VIOLATIONS OF:

(1) Confidentiality of Medical Information Act
(2) Invasion of Privacy
(3) Negligence
(4) Negligence Per Se
(5) Breach of Confidence
(6) Breach of Fiduciary Duty
(7) Unjust Enrichment
(8) California Unfair Competition Law
(9) Declaratory Relief

Jury Trial Demanded on All Causes of Action So Triable

Plaintiff Jane Roe 1 ("Plaintiff"),[1] brings this action on behalf of herself and all others similarly situated and for the benefit of the general public against the Sweetwater Union High School District ("SUHSD") and Does 1–25, inclusive (collectively referred to herein as "Defendants"). Plaintiff, through the undersigned counsel, alleges the following based on personal knowledge as to allegations regarding Plaintiff, and on information and belief as to all other allegations.

SUMMARY OF THE ACTION

1. As detailed more fully below, in February 2023 (and possibly earlier), SUHSD was subject to at least one cyber-attack and accompanying data breach and theft. This action arises from the negligent or reckless failure by SUHSD to adequately secure the private, personal, financial, and medical information of Plaintiff and all others similarly situated. The class as referred to herein is defined as all natural persons whose data was compromised and/or received or are to receive notice of this attack from SUHSD at some point from February 2023 (the "Class").

2. SUHSD abdicated its obligation and duty to protect sensitive personal information in its possession, as described in detail below, and failed to take steps necessary to prevent such an attack.

3. Based on information available to SUHSD, and in view of the known threat of 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 SUHSD's network and the failure to have in place basic antivirus and other software protections that would identify and/or alert SUHSD of an attack. To date, SUHSD so far has failed and refused to fully and adequately notify victims of this attack that their personal information was improperly accessed and stolen, the status of their information, and what actually was taken about them in full, leaving victims in the dark as to what they can and should do to protect themselves from further attacks that many have already suffered.

4. Defendants and their responsible contractors, subcontractors, representatives and/or employees negligently, recklessly, wantonly, or consciously created, maintained, preserved, and stored Plaintiff's and Class members' personally individually identifiable information, including "medical information" within the meaning of Cal. Civ. Code § 56.05(i), on an inadequately protected network.

[1] Due to the sensitive nature of this action, Plaintiff has chosen to file under a pseudonym. *See, e.g., Jane Doe 8015 v. Sup. Ct.,* 148 Cal.App.4th 489 (2007).

These actions proximately resulted in this damage and loss to Plaintiff and Class members as their medical, financial and/or personal information was improperly accessed and copied by unauthorized third parties.

5. In California, the protection of personal privacy is of paramount importance. Article 1, Section 1 of the California Constitution guarantees consumers their right to privacy. In addition, as recognized by the California State Legislature, the use of computer information technology has greatly magnified the potential risk to individual privacy that occurs from the maintenance of personal information by entities such as SUHSD, necessitating that the maintenance of personal information is subject to strict limits governed by numerous California statutes.[2]

6. Under California law, medical information is considered to be among the most sensitive private personal information available.[3] "Medical Information" is defined by California's Confidential Medical Information Act, Cal. Civ. Code sections 56, *et seq*. ("CMIA") as:

> any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment.
>
> "Individually identifiable" means that the Medical Information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or Social Security Number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual.[4]

7. "Personal and Medical Information," for purposes of this Complaint, refers to the above definition and encompasses both Personal Health Information ("PHI"), and Personally Identifiable Information ("PII"), including financial information such as banking information and Social Security numbers associated with individual student and employee records within SUHSD's computer systems.

8. Since Personal and Medical Information encompasses such personal and revealing information, it is highly valued as a gateway to medical identity theft[5] and general identity theft.[6] Personal

---

[2] *See* Cal. Civ. Code § 1798.1(b) & (c).
[3] *See, e.g.,* Cal. Civ. Code § 1798.140(ae)(2)(B) (as amended by Proposition 24) (defining health information as sensitive data).
[4] Cal. Civ. Code § 56.05(i).
[5] R. Kam, *et al, Medical Identity Theft: A Deadly Side Effect of Healthcare Data Breaches*, ID Experts (2017).
[6] Identity Theft Resource Center, *Data Breaches in the Healthcare Industry Continue Due to Availability of Valuable Information* (8/11/2020).

and Medical Information has been found to command up to $1,000 per individual record on the dark web.[7] Organizations such as SUHSD 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.

9. The threat of a cyberattack was reasonably foreseeable. School districts throughout California and the United States have been repeatedly warned of the potential for such an attack on their computer systems, and several districts in California have already been the subject of cyberattacks. SUHSD failed to implement reasonable and adequate security procedures to protect this data and failed to have in place basic antivirus and other software protections that would identify and/or alert SUHSD of an attack, or prevent such an attack in the first place.

10. Public entities and their service provider contractors or subcontractors are legally required and have a non-delegable duty to keep Personal and Medical Information in their possession, custody or control private and secured. Defendants breached duties owed to Plaintiff and Class members by, *inter alia*, (i) not exercising reasonable care in retaining, maintaining, securing, and safeguarding nonpublic Personal and Medical Information from being accessed and stolen by unauthorized persons; (ii) 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' security systems had been breached or improperly accessed; (iii) failing to timely disclose the facts surrounding this breach to Plaintiff and Class members; and (iv) failing to disclose that Defendants did not adequately secure Plaintiff's or Class members' Personal and Medical Information.

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

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

12. The Historical and Statutory Notes for the short title of the CMIA, § 56, support these reasonable expectations:

> The Legislature hereby finds and declares that persons receiving health care services have a right to expect that the confidentiality of individual identifiable Medical Information derived by health service providers be reasonably preserved. It is the intention of the Legislature in enacting this act, to provide for the confidentiality of individually identifiable Medical Information, while permitting certain reasonable and limited uses of that information.

Stats. 1981, ch. 782, § 1, p. 3040.

13. Additionally, Cal. Civ. Code § 56.101(a) states, in relevant part, that every entity that creates, maintains, preserves, is responsible for or stores Personal and Medical Information shall do so in a manner that preserves its confidentiality. Defendants' actions establish that they did not maintain the Personal and Medical Information at issue in a manner that preserved its confidentiality, as it was able to be improperly accessed and copied by unauthorized third parties. SUHSD's failure to create, maintain, preserve, and store Personal and Medical Information in a manner that preserved the confidentiality of the information contained therein resulted in the illegal access, authorization, exfiltration, disclosure, negligent release, and theft of data related to SUHSD employees and students, which necessarily included Personal and Medical Information.

14. Unfortunately for Plaintiff and Class members who either are or were enrolled with or employed by SUHSD, their Personal and Medical Information was not secured in the manner required under California law that would prevent such unauthorized access. What is worse, despite Defendants' obligations under law to promptly notify affected individuals so they can take appropriate action, Defendants (i) failed to do so without unreasonable delay, (ii) failed to include in the data breach notice a sufficient description of the data breach incident to comply with Cal. Civ. Code § 1798.29(d)(2)(E) and other relevant laws, and (iii) failed to provide in the data breach notice the information needed by Plaintiff and other similarly situated individuals to enable them to react appropriately to the breach, including taking whatever mitigation measures are necessary.

15. If a covered entity creates, maintains, preserves, or stores Personal and Medical Information in a negligent manner, it is subject to the remedies provided for under Cal. Civ. Code § 56.36(b).

16. The remedies provided for under Cal. Civ. Code § 56.36(b) allow private litigants to bring an action against an entity that has permitted the negligent release of confidential information or records or that failed to create, maintain, preserve, or store Personal and Medical Information in a manner that preserves its confidentiality to seek injunctive relief and, among other remedies, statutory damages of one thousand dollars ($1,000). To recover under this paragraph, it is not necessary that a plaintiff suffered or was threatened with actual damages. Cal. Civ. Code § 56.36(b)(1). These remedies are in addition to any other remedies available at law. Cal. Civ. Code § 56.36(b).

17. While reserving the right to assert claims for damages based on notice that has previously been provided to Defendants, Plaintiff is submitting a demand for the payment of damages to Defendants, which has not at this point been rejected but is likely futile. Plaintiff does not seek damages at this time but instead only injunctive and equitable relief until such time as Defendants have rejected Plaintiff's claims for damages, at which point she will amend this Complaint to seek such relief.

18. SUHSD failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information at issue in order to protect Plaintiff's and others' Personal and Medical Information. SUHSD also disclosed or permitted the disclosure of their Personal and Medical Information to unauthorized persons.

19. Defendants disregarded the rights of Plaintiff and members of the Class by negligently, recklessly, and consciously failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class members' Personal and Medical Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies, and procedures regarding data access and encryption, even for internal use, as well as appropriate procedures, such as two-step or multi-factor authentication, which would prevent such intrusions. As a result, the Personal and Medical Information of tens of thousands of Class members was compromised through disclosure to unknown and unauthorized third parties.

20. Plaintiff and Class members now face a long-term battle against identity theft as a result of this breach. Plaintiff and the Class members have a continuing interest in ensuring that this information is and remains safe. This presents an imminent and impending continuing risk for Plaintiff and Class members, particularly where SUHSD refuses to fully disclose any details of the attack and what data

were accessed and are available for third parties to exploit. SUHSD's failure to adequately protect the nonpublic Personal and Medical Information in their possession has likely caused, and will continue to cause, substantial harm and injuries to Plaintiff and Class members. Plaintiff and the Class are thus entitled to injunctive and other equitable relief.

21. Plaintiff brings this action seeking injunctive relief and equitable relief that is appropriate for the benefit of Plaintiff and the Class and the general public, including costs and expenses of litigation and attorneys' fees.

JURISDICTION AND VENUE

22. This Court has jurisdiction over this matter pursuant to Cal. Code Civ. Proc. § 410.10. The actions and conduct alleged in this Complaint took place in California, Plaintiff and Class members are primarily citizens of California, and Defendants conduct their operations in California and hold themselves out as a California state school district. Less than one-third of Class members are located outside of California.

23. Venue is proper in San Diego County pursuant to Cal. Code Civ. Proc. §§ 395 and 395.5 because a substantial part of the events and omissions giving rise to the claims occurred in this County as set forth herein, Plaintiff resides here, and Defendant SUHSD is based here and has significant operations in this County.

PARTIES

24. On personal knowledge, Plaintiff Jane Roe is a citizen and current resident of the State of California and is an employee of SUHSD and has been for several years. Plaintiff resides in San Diego County, California. Plaintiff, like each member of the Class, provided Defendants with Personal and Medical Information, as defined by Cal. Civ. Code § 56.05(i). The protection of Personal and Medical Information for both her and her family from unauthorized disclosure is important and material. Plaintiff received notification that she was a victim of this data breach on or about June 26, 2023. Plaintiff has experienced fear, anxiety, and worry caused by the unauthorized disclosure of Personal and Medical Information by SUHSD since she became aware of it. She remains concerned about the status of this information as she has not received full and complete notice from SUHSD 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 Medical Information for both her and her dependents. Plaintiff was personally impacted

and suffered damages and a loss of money or property as a result of this breach. 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. Plaintiff has received no compensation for the over 50 hours of time and effort she had to expend and will be required to expend to address this issue, independent of this litigation. She has just recently received notification that her personal information has been exfiltrated and has been improperly accessed, which she is unable to remedy on her own and she has no adequate remedy at law.

25. The Personal and Medical Information of Plaintiff Jane Roe was created, maintained, and preserved by and/or stored on Defendants' computer networks. Such Personal and Medical Information 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 could also contain medical record number, insurance provider, electronic mail address, telephone number, or other information that, alone or in combination with other publicly available information, reveals Plaintiff's identity.

26. Through the exfiltration of Personal and Medical Information that is associated with her and her family and that was illegally accessed by unauthorized third parties, Plaintiff has been injured in fact and lost money or property as a result of Defendants' misconduct in having her Personal and Medical Information disclosed to and stolen without her authorization, and the confidentiality and integrity of her Personal and Medical Information breached, lost, not preserved, and not protected.

27. Defendant SUHSD is a public agency that provides employment and educational services to residents of San Diego County. By acting in such a capacity and collecting Personal and Medical Information, SUHSD is or should be considered a "covered entity" for purposes of HIPAA.

28. The true names, roles, and capacities in terms of their involvement in the wrongdoing at issue, whether individual, corporate, associate, or otherwise, of Defendants named as Does 1 through 25, inclusive, are currently unknown to Plaintiff and, therefore, are named as Defendants under fictitious names pursuant to California Code of Civil Procedure Section 474. Plaintiff will identify these Defendants' true identities and their involvement in the wrongdoing at issue if and when they become known.

29. Defendants' conduct described herein, including reviewing, approving, or ratifying the conduct at issue, was undertaken as a supervising agency, agent, 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.

FACTUAL ALLEGATIONS

30. SUHSD is the largest secondary school district in California. It serves over 39,000 students and employs over 4,000 staff members across 32 schools in Chula Vista, Imperial Beach, National City and San Diego. It is also aware of the vulnerabilities of its computer systems, having had to disclose a data breach in October 2022 that had taken place on or about September 29, 2022. Significantly, SUHSD sent out notice of that breach within two weeks of that incident, showing it was aware of the importance of sending out prompt notice of a data breach to affected persons.

31. SUHSD initially reported a data breach of its systems in February 2023 about a possible cybersecurity incident impacting SUHSD, and sent out an email to SUHSD employees and students. That initial report specifically did not advise Plaintiff that her data had been compromised, and she did not discover she had been a victim of this data breach. Plaintiff did not receive a letter notifying her she was a victim of this breach until on or about July 2, 2023 at the earliest.

32. Dr. Moises Aguirre, Superintendent of SUHSD, originally said in an email to employees and parents of SUHSD on or about February 24, 2023 with the vague subject line "Systems Status Update" that:

> on February 12, 2023, we became aware of an incident that has impacted the availability of certain systems, including email, within our network. We immediately launched an investigation. As part of that investigation, we will be shutting down internet access to certain of our systems. You will still be able to access some Sweetwater applications from systems not connected to our network, such as home computers or other personal devices connected to the internet at home or outside of the school district buildings. We understand this will be inconvenient, but we are focused on securely restoring our systems as quickly and as safely as possible. We are working quickly to determine what occurred in addition to restoring services. *While our investigation is in the early stages, to the extent the investigation determines that any individuals' personal information was accessed or*

acquired, we will communicate directly with those individuals.

No other details were provided, other than an offer to sign up for a year of credit monitoring (notably Plaintiff requested but did not receive confirmation SUHSD actually had signed her up for this service). As indicated by this letter, there was no notification that individuals' Personal and Medical Information had actually been compromised.

33. However, in a letter dated June 15, 2023 but not sent out until the end of June 2023 and that was just received by Plaintiff, SUHSD claimed it discovered the breach on or about February 25, 2023 when it experienced network outages that disrupted online learning and other operations. Apparently between February 11 and 12, 2023, an unauthorized person gained access to SUHSD's computer network and took files that contained the personal information of an unknown number of people, including employees' dependents. SUHSD hired a cybersecurity firm to investigate the incident and found that an unauthorized third party had accessed its network and encrypted some of its files. Defendants admitted that at some undetermined point in time that the intruder had also exfiltrated data from its servers. SUHSD has failed to disclose the precise nature of the data that was exfiltrated, but considering the servers that were accessed, the person who obtained unauthorized access took files that either included or could have included names, dates of birth, Social Security numbers, addresses, phone numbers, email addresses, student ID numbers, grades, transcripts, attendance records, discipline records, health information, and/or payroll information of current and former students and employees.

34. In a June 23, 2023 statement, SUHSD said it has implemented safeguards and technical security measures "(t)o prevent something like this from happening again." It is unclear whether the District had any cybersecurity measures in place prior to the data breach and if it paid any form of ransom or was subject to a ransomware attack. In March 2023 it announced it had hired three organizations (Baker & Hostetler LLP, Kroll and Cypfer, Inc.), to investigate the incident and provide security advice for an amount not to exceed $75,000. In April 2023, the District also entered into an agreement with Logicalis for its multi-factor authentication software so that employees could prevent unauthorized access to district systems. According to that contract, the term of the software is for one year at a cost of $58,708. This disclosure was significant, because it suggests SUHSD did not have such basic security measures in place prior to this attack and breach, despite being on notice of the potential for an attack

and a breach that had taken place just months earlier.

35. SUHSD has released very few details about the actual incident, only referring members of the public to the breach letter that itself failed to include critical information, but only would say that its systems were operational and there was no impact on their safety and emergency mechanisms at any schools or offices. Medical information has also apparently been implicated for some individuals, but it was not clear from the description of the breach how many people have had their health information compromised and SUHSD has failed to inform Plaintiff and others if their medical information was compromised. The sample data breach letter filed with the Attorney General's office by SUHSD confirmed that the cybersecurity incident occurred on or about February 12, 2023 – almost five months before the first notification to employees and student families they were victims of this incident.

36. The letter included in SUHSD's filing with the California Attorney General states that SUHSD has implemented additional security measures to enhance our existing cybersecurity protocols but does not specify what those measures include. Also, SUHSD confirmed in the letter that it would offer a complimentary one-year membership to an identity monitoring service for victims of this breach, significantly less than what the law requires.

37. For some reason, the number of individuals affected by this breach has still not been fully disclosed by SUHSD but is now likely in the tens of thousands of individuals as it involved many former and current SUHSD employees and students.

38. The fact SUHSD has waited for months to advise impacted individuals of this issue has caused significant harm. The longer cyber thieves can go undetected, the more they stand to profit from their illegal activities. Personal data about minor students, which may include special education information and other highly sensitive materials, should be robustly protected by school districts. And had Plaintiff been timely informed of this breach she could have placed alerts on file with her financial institution and relevant credit reporting agencies.

39. Not only did SUHSD fail to provide a general description of the breach incident as required for purposes of statutory compliance, its vague and obfuscating language unfairly prevents those individuals who have been victimized in this attack from having sufficient information to take specific actions and mitigating measures that they might otherwise choose to if they were provided even the basic

facts. What's worse, at least one recipient of this letter reported that as she looked closer at the letter she received, she noticed it was sent to her address, but it had another person's name. "It wasn't for me; it was for a student, but it had my home address on it. I'm assuming it's a student, it could be another employee," said the employee. She reported the incident to the District Superintendent, who simply stated he would look into it.

40. These are significant discrepancies. For example, it would likely make a material difference to a consumer if his or her Personal and Medical Information was compromised by a group of teenagers, or researchers trying to alert SUHSD that its security systems are deficient, as opposed to that sensitive data being stolen by a gang of cyber-thieves. Knowledge that the latter has occurred highlights the need to take as many mitigation measures as possible and scrutinize future financial and medical statements for evidence of identity theft. SUHSD employees and students have not received disclosure of these material facts.

41. Plaintiff by and through counsel is submitting to SUHSD the form Notice of Claims required by SUHSD. It is likely this submission will be futile and thus can be excused. Plaintiff will amend this Complaint upon the resolution of that Notice of Claims submission.

A. Defendants Were on Notice of The Potential for Unauthorized Access To Their Servers

42. SUHSD has been previously placed on notice of the potential for such an attack on its systems but did not take sufficient steps to prevent it and failed to have in place basic antivirus and other protections that would have notified it of such an attack and/or prevented it altogether.

43. Defendant SUHSD's negligence or reckless or conscious disregard of its obligations to safeguard the Personal and Medical Information of Plaintiff and the Class members was exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data, especially in light of the substantial increase in cyberattacks and data breaches of school districts throughout California and the United States preceding the date of this attack.

44. Despite requests to Defendants to take appropriate action prior to the filing of this Complaint, to date this unauthorized access, disclosure, and exfiltration remains fully unremedied. Defendants failed to provide notice to affected consumers in the most expedient time possible and without

unreasonable delay, as required under California law, nor did it provide complete and accurate notice.

45. Defendants knew, or reasonably should have known, the importance of safeguarding the Personal and Medical Information entrusted to them and of the foreseeable consequences if their computer network was breached. Defendants were on notice that they should have and could have prevented this attack by properly securing and encrypting the Personal and Medical Information of Plaintiff and the Class members and taking the steps outlined above to prevent infiltration by common methods such as phishing by, for example using multi-factor authentication. Defendants could also have destroyed data of former employees and students that was no longer useful, especially outdated data. Defendants failed, however, to take adequate measures to prevent this foreseeable attack.

46. Indeed, similar cyberattacks have become so notorious that the FBI and U.S. Secret Service back in 2019 issued a warning to potential targets such as SUHSD so they are aware of, and prepared for, a potential attack. As one report explained in an ominous foreshadowing of the events here, "[e]ntities like smaller municipalities and hospitals are attractive … because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[8]

47. The increase in such attacks, and the attendant risk of future attacks, was widely known within Defendant SUHSD's industry. Due to the high-profile nature of these breaches and attacks, Defendants either were or should have been on heightened notice and aware of such attacks occurring within school districts and, therefore, should have been on notice of their duty to be proactive in guarding against being subject to such attacks and adequately performed their duty of overseeing, preparing for, and immediately identifying such an attack.

48. Yet, despite the prevalence of public announcements about these data breach and data security compromises and Defendants' preparations for them, Defendants failed to insist their agents and employees take appropriate steps to protect Plaintiff's and Class members' Personal and Medical Information from being compromised and failed to timely, properly, and appropriately notify such persons that such an attack had taken place and the nature of the exfiltrated data.

[8] *See*, FBI, Secret Service Warn of Targeted Ransomware, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last accessed 5/3/22)

B. Defendants Had an Obligation to Protect Personal And Medical Information Under State And Federal Law And The Applicable Standard of Care

49. Defendants are required by the CMIA, HIPAA and various other laws and regulations to protect Plaintiff's and Class members' Personal and Medical Information and to handle notification of any breach in accordance with applicable breach notification statutes. Defendants also needed to or should segment data by, among other things, 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. Failing to do so results in acts of negligence *per se* by Defendants. These duties are established in numerous California statutes, including Cal. Civ. Code §§ 56.101, 1798.21, and 1798.26.

50. In addition, as Defendants are entities either directly or indirectly covered by HIPAA, they are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and 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 Personal and Medical Information maintained by them in electronic form.

51. 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.

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

53. 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.

54. 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 also 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).

55. The attack on Defendants, particularly in light of the information that was available and should have been reviewed by them almost a year before the attack, establishes they did not comply with these Rules. This attack resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations, including, but not limited to, the following:

(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 persons or software programs that have been granted access rights, in violation of 45 C.F.R. section 164.312(a)(1);

(c) Failing to implement policies and procedures 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, to the extent practicable, harmful effects of security incidents that are 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 anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding 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 persons, 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 with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain 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).

56. 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 pursuant to that Act has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.[9] This duty extends to Defendants as responsible for the actions or inactions of their exclusive contractor or subcontractor.

57. As established by these laws, Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal and Medical Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants also owed a duty to Plaintiff 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 Personal and Medical Information and were not exposed to unauthorized third parties. This also included a duty to Plaintiff and Class members to design, maintain, and test their computer systems to ensure that the Personal and Medical Information in their possession was adequately secured and protected; to create and implement reasonable data security practices and procedures to protect the Personal and Medical Information in their possession and avoid access to their systems through processes such as phishing,

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

including adequately training employees and others who accessed information within their systems on how to adequately protect Personal and Medical Information; avoid permitting such infiltration such as by use of multi-factor authentication; to implement processes that would detect a breach of their data security systems in a timely manner and to act upon data security warnings and alerts in a timely fashion; to disclose if their computer systems and data security practices were inadequate to safeguard individuals' Personal and Medical Information from theft or exfiltration; and to disclose in a timely and accurate manner when data breaches or cyberattacks occurred.

58. Defendants owed these duties to Plaintiff and Class members because they were foreseeable and probable victims of any inadequate data security practices. Defendants affirmatively chose to design their systems with inadequate 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 being able to execute the attack and exfiltrate the data in question, to the injury and detriment of Plaintiff and Class members. By taking affirmative acts inconsistent with these obligations that left SUHSD's computer system vulnerable to attack, Defendants disclosed and permitted the disclosure of Personal and Medical Information to unauthorized third parties. Through such actions or inactions, SUHSD failed to preserve the confidentiality of Personal and Medical Information they were duty-bound to protect.

59. As a direct and proximate result of Defendants' actions, inactions, omissions, breaches of duties and want of ordinary care that directly and proximately caused or resulted in the cyberattack and the resulting data breach, Plaintiff 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 and effort they are required to expend, (b) invasion of privacy, (c) breach of the confidentiality of their Personal and Medical Information and costs and time associated with remedying such breaches, (d) deprivation of the value of their PHI, for which there is a well-established national and international market, as well as statutory damages to which they are entitled even without proof of access or actual damages; (e) the financial and temporal cost of monitoring their credit reports and financial accounts, and (f) increased

risk of future harm.

C. The Value of Personal And Medical Information Shows That Plaintiff And Others Lost Valuable Money or Property as a Result of This Unauthorized Access

60. It is well known that Personal and Medical Information is a valuable commodity[10] and the frequent target of hackers, such that Plaintiff and Class members would lose money or property if their data was permitted to be improperly accessed or stolen.

61. Defendants either were or should have been aware that the Personal and Medical Information they collect 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 identify theft, medical and financial fraud.[11]

62. Indeed, a robust black market exists in which criminals post stolen Personal and Medical Information on multiple underground Internet websites, commonly referred to as the dark web, to create fake insurance claims, purchase and resell medical equipment, or access prescriptions for illegal use or resale. Criminals often trade stolen Personal and Medical Information on the "cyber black market" for years following a breach. For example, it is believed that certain Personal and Medical Information compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits.[12] According to a 2017 Javelin strategy and research presentation, fraudulent activities based on data stolen in data breaches that are between two and six years old had increased by nearly 400% over the previous 4 years.[13]

63. 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 upon completeness.[14] PII and PHI can be sold

---

[10] *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*).

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

[12] 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 accessed 5/3/22).

[13] *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 accessed 5/3/22).

[14] *Id.*

at a price ranging from approximately $20 to $300.[15]

64. The Ponemon Institute found that medical identity theft can cost victims an average of $13,500 to resolve per incident and that victims often have to pay off the imposter's medical bills to resolve the breach.[16]

65. In another study by the Ponemon Institute in 2015, 31% of medical identity theft victims lost their healthcare coverage as a result of the incident, while 29% had to pay to restore their health coverage, and over half were unable to resolve the identity theft at all.[17]

66. Once Personal and Medical Information 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 such data resulting from the attack may not come to light for years. 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."[18] The ramifications of Defendants' failure to keep the Medical Information and Personal Information in question secure from attack and then not advise affected persons of all the relevant facts is thus not temporary but long lasting, as the fraudulent use of that information and damage to victims may continue for years. That is one of the reasons providing prompt, accurate and fulsome notice to consumers as expeditiously as possible is necessary, so they can take actions to protect themselves. Yet Defendants are still refusing to even acknowledge the extent of the attack that took place, let alone provided timely, proper, and appropriately comprehensive notice in the most expedient time possible and

[15] https://www.privacyaffairs.com/dark-web-price-index-2021/

[16] 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 accessed 5/3/22).

[17] 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 accessed 5/3/22).

[18] *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 accessed 5/3/22).

without unreasonable delay, as required under California law.

67. Plaintiff served demands for damages, both for herself and all others similarly situated, that Defendants may insist were required to assert claims for damages against public agencies under Government Code Section 915(a). Without waiving arguments such claims were not required or that multiple demands were required for each individual Plaintiff as any further claims would be futile, Plaintiff has satisfied any requirement to submit such claims, making any claims by other potential plaintiffs or Class members futile and thereby exhausted.

CLASS ALLEGATIONS

68. Plaintiff, on behalf of herself and all others similarly situated, bring this action pursuant to California Code of Civil Procedure Section 382. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements for class certification.

69. The Class is defined in Paragraph 1 above. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether class certification is appropriate.

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

71. 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 bases underlying Defendants' misconduct is common to all Class members and represent a common thread of unlawful and negligent conduct, resulting in injury to all members of the Class. These common legal and factual questions include the following:

(a) Whether SUHSD implemented and maintained reasonable security practices and procedures appropriate to protect Plaintiff's and Class members' Personal and Medical Information from unauthorized access, destruction, use, theft, modification, or disclosure;

(b) Whether Defendants and their contractors, subcontractors, employees, agents, officers, or directors negligently or unlawfully disclosed or permitted the unauthorized disclosure of Plaintiff's and Class members' Personal and Medical Information to

unauthorized persons or provided negligent oversight of the actions of SUHSD;

(c) Whether SUHSD had taken steps to ensure it had not negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and Class members' Personal and Medical Information, and failed to protect and preserve the integrity of the Personal and Medical Information found on SUHSD'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 Plaintiff and the Class;

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

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

(g) Whether Defendants engaged in "unfair" business practices by failing to safeguard the Personal and Medical Information of Plaintiff and the Class, and whether Defendants' violations of the state and federal laws cited herein constitute "unlawful" business practices in violation of California Business and Professions Code § 17200, et seq.;

(h) Whether Defendants violated the California Medical Information Act, the Student Online Personal Information Protection Act, and the other laws cited herein; and

(i) Whether Plaintiff and the Class are entitled to relief to redress the imminent and currently ongoing harm faced as a result of the cyberattack and Defendants' failure to provide full and adequate notice thereof, and the scope of such relief.

72. Plaintiff's claims are typical of the claims of other Class members. There is no unique defense available to Defendants as Plaintiff, like all Class members, was part of SUHSD and was apparently subjected to the unauthorized disclosure of Personal and Medical Information as a result of Defendants' conduct.

73. Plaintiff will fairly and adequately represent the interests of the Class members. Plaintiff

has retained counsel with substantial experience in prosecuting complex litigation and class actions, including data breaches concerning the sensitive Personal and Medical Information of individuals. Plaintiff and counsel are committed to vigorously prosecuting the action on behalf of the Class. Neither Plaintiff nor counsel has any interest adverse to or that irreconcilably conflicts with those of other Class members.

74. Absent a class action, most members of the Class would find the cost of litigating their claims to be prohibitive and may have no effective and complete remedy and may not even learn of the 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. Plaintiff thus anticipates no difficulty in the management of this case as a class action and providing notice to members of the Class.

75. 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.

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

CAUSES OF ACTION

FIRST CAUSE OF ACTION

VIOLATION OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT

Cal. Civ. Code § 56 *et seq*.

77. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein. This Cause of Action is brought on behalf of all persons who had their Medical Information compromised as a result of the unauthorized access of data as set forth herein, which would include Social Security numbers for purposes of this Cause of Action.

78. Defendant SUHSD is subject to the requirements of the CMIA.

79. SUHSD must not disclose or permit the disclosure of Personal and Medical Information

without first obtaining authorization, subject to certain exceptions found in Cal. Civ. Code §§ 56.10(b) & (c) that do not apply here. Cal. Civ. Code § 56.10(a). By their affirmative acts and inactions set forth above, Defendants disclosed or permitted the disclosure of Personal and Medical Information to unauthorized third parties, in violation of this Section.

80. SUHSD is required under the CMIA to ensure that it maintains, preserves, and stores Personal and Medical Information in a manner that preserves the confidentiality of the information contained therein. Cal. Civ. Code §§ 56.101(a) & 56.36(b).

81. SUHSD is required to create, maintain, preserve, store, abandon, destroy, or dispose of Personal and Medical Information in a non-negligent manner. Cal. Civ. Code § 56.101(a).

82. Under the CMIA, persons who hold or have access to electronic health record systems or electronic medical record systems are required to protect and preserve the integrity of electronic Personal and Medical Information. Cal. Civ. Code § 56.101(b)(1)(A). The term "electronic health record" or "electronic medical record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized healthcare clinicians and staff. Cal. Civ. Code § 56.101(c) as defined by 42 U.S.C. § 17921(5).

83. Plaintiff and members of the Class are "Patients" as defined by Cal. Civ. Code section 56.05(j).

84. As described above, the actions or inactions of SUHSD failed to preserve the confidentiality of Personal and Medical Information, including but not limited to Plaintiff's and Class members' full names, dates of birth, addresses, Social Security numbers, as well as potentially insurance provider and health program participant information that, either alone or in combination with other publicly available information, reveals their identities.

85. The Personal and Medical Information that was the subject of the attack and resulting data breach detailed above was accessed, removed, and viewed by unauthorized parties during and following the attack.

86. As this data was specifically exfiltrated by a person who did not have access to the SUHSD servers, the unauthorized persons necessarily viewed the data at issue herein and the confidentiality and integrity of that data was breached, lost, not preserved, and not protected by

Defendants.

87. In violation of the CMIA, Defendants disclosed or permitted the disclosure of Personal and Medical Information regarding Plaintiff and Class members without authorization to a third party. This disclosure did not qualify for any of the exemptions set forth in Cal. Civ. Code §§ 56.10(b) or (c), which provide limited bases for allowing unauthorized disclosures. This disclosure of Personal and Medical Information to unauthorized individuals resulted from the affirmative actions and inactions of Defendants and their employees.

88. In violation of the CMIA, Defendants failed to ensure that SUHSD created, maintained, preserved, stored, abandoned, destroyed, or disposed of Personal and Medical Information of Plaintiff and Class members in a manner that preserved the confidentiality of the information contained therein.

89. In violation of the CMIA, Defendants failed to ensure that SUHSD created, maintained, preserved, stored, abandoned, destroyed, or disposed of Personal and Medical Information of Plaintiff and Class members in a non-negligent manner.

90. In violation of the CMIA, Defendants failed to ensure that SUHSD's electronic health record systems or electronic medical record systems would protect and preserve the integrity of Plaintiff's and Class members' Personal and Medical Information.

91. In violation of the CMIA, Defendants negligently released confidential information or records concerning Plaintiff and Class members, either directly or through the acts of its exclusive contractor or subcontractor.

92. In violation of the CMIA, Defendants failed to ensure that SUHSD give prompt, timely, and fulsome notice of the attack and resulting data breach.

93. As a direct and proximate result of Defendants' wrongful actions, inactions, omissions, and want of ordinary care that directly and proximately caused the release of Personal and Medical Information of tens of thousands of individuals, such Personal and Medical Information was viewed by, released to, and disclosed to third parties without appropriate written authorization.

94. Plaintiff and Class members are therefore entitled to injunctive relief and reasonable attorneys' fees and costs.

95. Plaintiff served demands for monetary relief that Defendants assert are required by law.

If Defendants reject Plaintiff's claims for payment of damages, Plaintiff will seek actual damages for Class members, statutory damages of $1,000 per Class member and punitive damages of $3,000 per Class member.

SECOND CAUSE OF ACTION

INVASION OF PRIVACY

California Constitution, Article I, Section 1

96. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

97. The California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const., Art. I., § 1.

98. Plaintiff and Class members had a legitimate expectation of privacy in their Personal and Medical Information, and were entitled to the protection of this information against disclosure to unauthorized third parties.

99. Defendants owed a duty to Plaintiff and Class members to keep their Personal and Medical Information confidential.

100. Defendants failed to protect against any release to unauthorized third parties the non-redacted and non-encrypted Personal and Medical Information of Plaintiff and Class members.

101. Defendants allowed unauthorized and unknown third parties access to and examination of the Personal and Medical Information of Plaintiff and Class members by way of Defendants' affirmative actions and negligent failures to protect this information through the negligent oversight of SUHSD.

102. The unauthorized release to, custody of, and examination by unauthorized third parties of the Personal and Medical Information of Plaintiff and Class members is highly offensive to a reasonable person.

103. The intrusion at issue was into a place or thing, which was private and is entitled to be private. Plaintiff and Class members disclosed their Personal and Medical Information to Defendants as part of Plaintiff's and Class members' relationships with Defendants, but privately and with the intention

that the Personal and Medical Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

104. The attack that resulted from the actions and inactions of Defendants either directly or through the actions and inactions of SUHSD employees constitutes an intentional interference with Plaintiff's and Class members' interest in solitude or seclusion, 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.

105. Defendants acted with a knowing or negligent state of mind when they permitted the attack described herein to occur, because they either knew or reasonably should have known that their information and data security practices were inadequate, that they did not have basic antivirus or other software systems in place, and that their existing systems were insufficient to protect against such attacks.

106. Defendants either knew or reasonably should have known that SUHSD's inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class members.

107. As a proximate result of the above acts and omissions of Defendants, the Personal and Medical Information of Plaintiff and Class members was disclosed to third parties without authorization, causing Plaintiff and Class members to suffer injuries and damages.

108. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause irreparable injury to Plaintiff and the Class, entitling them to seek injunctive relief.

109. This action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons and the general public. Private enforcement is necessary and places a disproportionate financial burden on Plaintiff in relation to Plaintiff's stake in the matter. Because this case is brought to enforce important rights affecting the public interest, Plaintiff also seeks the recovery of attorneys' fees and costs in prosecuting this action against Defendants under Cal. Code Civ. Proc. § 1021.5 and other applicable law.

THIRD CAUSE OF ACTION

NEGLIGENCE

110. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

111. Defendants collected, came into possession of, and maintained Plaintiff's and Class members' Personal and Medical Information, 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.

112. Defendants had a special relationship with Plaintiff and Class members who entrusted Defendants with adequately protecting their Personal and Medical Information.

113. Defendants knew that the Personal and Medical Information was private and confidential and should be protected as private and confidential, and thus, Defendants owed a duty of care not to subject Plaintiff and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

114. Defendants knew, or should have known, of the risks inherent in collecting and storing Personal and Medical Information, the vulnerabilities of SUHSD's data security systems, and the importance of adequate security.

115. Defendants knew, or should have known, of SUHSD's heightened vulnerability, to cyber-attacks and breaches by cybercriminals. Defendants knew or should have known about the threat posed to it. Defendants' failure to ensure SUHSD take proper security measures to protect Plaintiff and Class member's Personal and Medical Information created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of Personal and Medical Information by unauthorized third parties. As described above, given that school districts such as SUHSD were known at the time of the attack to be prime targets for hackers Plaintiff and Class members are part of a foreseeable, discernable group that was at high risk of having their Personal and Medical Information compromised, exfiltrated, and otherwise wrongly disclosed if not adequately protected by Defendants.

116. It was also foreseeable that Plaintiff and Class members would sustain injuries if SUHSD failed to provide timely, direct, understandable, and complete notice of this data breach to Plaintiff and

Class members.

117. Defendants had a duty to ensure that SUHSD employees would employ reasonable security measures, systems, processes, and otherwise protect the Personal and Medical Information of Plaintiff and Class members pursuant to the state and federal laws set forth above, resulting in Defendants' liability under principles of negligence.

118. Defendants had a duty to ensure that SUHSD 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 cyber-attacks.

119. Defendants owed a duty to ensure that SUHSD would timely and adequately inform Plaintiff and Class members, in the event of a data breach, that their Personal and Medical Information had been compromised or improperly disclosed as part of a cyberattack to unauthorized third parties.

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

121. Defendants, through their actions and omissions, unlawfully breached duties to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class members' Personal and Medical Information within Defendants' possession, supervision, and control.

122. Defendants, through their actions and omissions, unlawfully breached duties owed to Plaintiff and Class members by failing to ensure that SUHSD would have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class members' Personal and Medical Information.

123. Defendants, through their actions and omissions, unlawfully breached duties to ensure that SUHSD would timely and fully disclose to Plaintiff and Class members that the Personal and Medical Information within Defendants' possession, supervision, and control was compromised, the nature of the compromise, and precisely the type of information compromised.

124. Defendants' breach of duties owed to Plaintiff and Class members proximately caused Plaintiff's and Class members' Personal and Medical Information to be compromised and suffer losses, including direct economic losses.

125. As a result of Defendants' ongoing failure to adequately notify Plaintiff and Class

members regarding what type of Personal and Medical Information has been compromised, Plaintiff and Class members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

126. Defendants' breaches of duty caused Plaintiff and Class members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Personal and Medical Information.

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

128. Plaintiff seeks 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 personal and medical information and provide full and complete notice to all affected persons, as set forth below.

FOURTH CAUSE OF ACTION

NEGLIGENCE PER SE

129. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

130. Pursuant to the laws set forth herein, including Cal. Civ. Code § 56.10(a), 56.101, 1798.21, 1798.29, the Student Online Personal Information Protection Act, Bus. & Prof. code Section 22584 et seq. ("SOPIPA"), and Article I, § 1 of the California Constitution, Defendants' actions or inactions described above also violated federal statutes and regulations, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and 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 and the other sections identified above, Defendants were required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class members' Personal and Medical Information.

131. Plaintiff and Class members are within the class of persons that these statutes and rules

were designed to protect.

132. Defendants breached the duties established by those laws by failing to ensure that SUHSD would employ industry standard data and cybersecurity measures to ensure compliance with those laws, including, but not limited to, proper segregation, access controls, two-factor authentication, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

133. 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 Plaintiff's and Class members' Personal and Medical Information in compliance with applicable laws would result in an unauthorized third-party gaining access to SUHSD's networks, databases, and computers that stored or contained Plaintiff's and Class members' Personal and Medical Information resulting in Defendants' liability under principles of negligence *per se*.

134. Plaintiff's and Class members' Personal and Medical Information constitutes personal property that was stolen as a proximate result of Defendants' negligence, resulting in harm, injury and damages to Plaintiff and Class members.

135. Defendants' conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class members' Personal and Medical Information and Plaintiff and Class members have suffered and will continue to suffer damages as a result of Defendants' conduct.

FIFTH CAUSE OF ACTION

BREACH OF CONFIDENCE

136. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

137. At all times during Plaintiff's and Class members' interactions with SUHSD, Defendants were required to ensure that SUHSD would be aware of the confidential and sensitive nature of Plaintiff's and the Class members' Personal and Medical Information that Plaintiff and Class members provided to Defendants.

138. As alleged herein, Defendants' relationship with Plaintiff and Class members was

governed by the reasonable expectations that Plaintiff's and the Class members' Personal and Medical Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

139. Plaintiff and Class members provided their Personal and Medical Information with the explicit and implicit understandings that it would be protected and that such Personal and Medical Information would not be disseminated to any unauthorized third parties, and that the persons who had access to such data would take precautions to protect that Personal and Medical Information from unauthorized disclosure.

140. Defendants voluntarily received in confidence Plaintiff's and Class members' Personal and Medical Information with the understanding that such information would not be disclosed or disseminated to the public or any unauthorized third parties.

141. As a proximate result of Defendants' failure to prevent and avoid the attack and resulting data breach at issue here, Plaintiff's and Class members' Personal and Medical Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class members' confidence, and without their express permission.

142. As a direct and proximate cause of Defendants' actions and omissions as detailed above, Plaintiff and the Class members have suffered injury and harm.

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

144. The injury and harm Plaintiff and the Class members suffered was the reasonably foreseeable result of Defendants' conduct, which permitted the unauthorized disclosure of Plaintiff's and Class members' Personal and Medical Information. Defendants either knew, or should have known, that SUHSD's methods of accepting and securing Plaintiff's and the Class members' Personal and Medical Information was inadequate as it relates to, at the very least, securing servers and other computer

equipment solely the responsibility of SUHSD and containing Plaintiff's and Class members' Personal and Medical Information.

145. As a direct and proximate result of Defendants' breaches of confidence to Plaintiff and Class members, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft or compromise; (ii) the loss of the opportunity how their Personal and Medical Information is used; (iii) the compromise, publication, and theft of their Personal and Medical Information; (iv) time and expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and unauthorized use of their Personal and Medical Information, such as set forth for Plaintiff above; (v) 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; (vi) costs associated with placing freezes or monitoring on credit reports; (vii) the continued risk to their Personal and Medical Information, 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 Personal and Medical Information of current and former students and employees and their beneficiaries and dependents; and (viii) 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 Personal and Medical Information compromised as a result of the attack.

146. Plaintiff seeks 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 protected information, as set forth below.

SIXTH CAUSE OF ACTION

BREACH OF FIDUCIARY DUTY

147. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

148. Plaintiff and Class members gave Defendants their Personal and Medical Information in confidence, believing that Defendants would protect that information. Plaintiff and Class

members would not have provided Defendants with this information had they known it would not be adequately protected.

149. Defendants' acceptance and storage of Plaintiff's and Class members' Personal and Medical Information as well as, for Plaintiff and many members of the Class, their status as employees and students of SUHSD, created a fiduciary relationship between Defendants and Plaintiff and Class members. In light of this relationship, Defendants must act primarily for the benefit of such persons, which includes safeguarding and protecting Plaintiff's and Class Members' Personal and Medical Information.

150. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' Personal and Medical Information, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' Personal and Medical Information that it collected.

151. As a direct and proximate result of Defendants' breaches of fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft or compromise; (ii) the loss of the opportunity how their Personal and Medical Information is used; (iii) the compromise, publication, and theft of their Personal and Medical Information; (iv) time and expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and unauthorized use of their Personal and Medical Information, such as set forth for Plaintiff above; (v) 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; (vi) costs associated with placing freezes or monitoring on credit reports; (vii) the continued risk to their Personal and Medical Information, 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 Personal and Medical Information of current and former

students and employees and their beneficiaries and dependents; and (viii) 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 Personal and Medical Information compromised as a result of the attack.

152. Plaintiff seeks 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 protected information, as set forth below.

SEVENTH CAUSE OF ACTION

UNJUST ENRICHMENT

153. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder and is plead in the alternative to other claims for relief.

154. Defendants benefited from either directly or indirectly receiving Plaintiff's and Class members' Personal and Medical Information by their ability to retain and use that information for their own benefit. Defendants understood this benefit.

155. Defendants also understood and appreciated that Plaintiff's and Class members' Personal and Medical Information was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that information.

156. Defendants failed to ensure that SUHSD would expend the resources necessary to provide reasonable security, safeguards, and protections to the Personal and Medical Information of Plaintiff and Class members. SUHSD is liable to all persons impacted by this breach for the damage caused by this data breach incident and for unjust enrichment from the monies they saved by not having adequate security systems in place.

157. Under the 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.

158. Defendants wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class members.

159. Defendants' enrichment at the expense of Plaintiff and Class members is and was unjust.

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

EIGHTH CAUSE OF ACTION

VIOLATION OF THE UNFAIR COMPETITION LAW

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

161. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

162. The acts, misrepresentations, omissions, practices, and non-disclosures of Defendants as alleged herein constituted unlawful and unfair business acts and practices within the meaning of Cal. Bus. & Prof. Code §§ 17200, *et seq*.

163. Defendants engaged in "unlawful" business acts and practices in violation of the California statutes set forth above, including Cal. Civ. Code §§ 56.10(a), 56.101, 1798.21, 1798.29 and Article I, § 1 of the California Constitution. The Student Online Personal Information Protection Act, Bus. And Prof Code Section 22584 *et seq*., requires that every online service used primarily for primary and secondary school purposes must maintain reasonable security procedures and practices to protect student personal information from unauthorized access, destruction, or disclosure. Defendants' acts also violated federal statutes and regulations, including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and 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 and the other sections identified above. Plaintiff reserves the right to allege other violations of law committed by Defendants that constitute unlawful business acts or practices within the meaning of Cal. Bus. & Prof. Code §§ 17200, *et seq*.

164. Defendants have also engaged in "unfair" business acts or practices. There are several tests that determine whether a practice that impacts consumers as compared to competitors is "unfair," examining the practice's impact on the public balanced against the reasons, justifications and motives of Defendants. Defendants' conduct would qualify as "unfair" under any of these standards:

(a) whether the practice offends an established public policy, which here is whether

the practices at issue offend the policies of protecting consumers' Personal and Medical Information by engaging in illegal practices, as reflected in California law and policy set forth above;

(b) balancing the utility of Defendants' conduct against the gravity of the harm created by that conduct, including whether Defendants' practices caused substantial injury to consumers with little to no countervailing legitimate benefit that could not reasonably have been avoided by the consumers themselves, and causes substantial injury to them; or

(c) whether the practice is immoral, unethical, oppressive, unscrupulous, unconscionable or substantially injurious to consumers.

165. The harm caused by Defendants' failure to ensure that SUHSD would maintain adequate information security procedures and practices, including, but not limited to, failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions, failing to properly and adequately educate and train employees, failing to put into place reasonable or adequately protected computer systems and security practices to safeguard employees and students' Personal and Medical Information, including access restrictions, multi-factor authentication and encryption, failing to have adequate privacy policies and procedures in place that did not preserve the confidentiality of the Personal and Medical Information of Plaintiff and the Class members in their possession, failing to timely and accurately disclose the cyberattack and resulting data breach to Plaintiff and Class members, and failing to protect and preserve confidentiality of Personal and Medical Information of Plaintiff and Class members against disclosure and release, outweighs the utility of such conduct and such conduct offends public policy, is immoral, unscrupulous, unethical, and offensive, and causes substantial injury to Plaintiff and Class members.

166. Defendants either knew or should have known that SUHSD's data security and protection practices were inadequate to safeguard the Personal and Medical Information of Plaintiff and Class members, deter cyberthieves, and detect an attack and resulting data breach within a reasonable time, even though the risk of a data breach or theft was highly likely, especially given Defendants had been on notice for almost a year of the potential for an attack on its systems. The business acts and practices by

Defendants for failure to keep confidential medical, demographic, or personal data protected, encrypted and without sufficient security to be breached by an adverse third party did not meet all applicable standards of care and vigilance.

167. These unlawful and unfair business acts or practices conducted by Defendants have been committed in the past and continue to this day. Defendants have failed to fully acknowledge the wrongful nature of their actions. Defendants have not corrected or publicly issued comprehensive corrective notices to Plaintiff and the Class members and may not have corrected or enacted adequate policies and procedures to protect and preserve confidentiality of medical and personal identifying information of Plaintiff and the Class in their possession.

168. As set forth above, Plaintiff has been injured in fact and lost money or property as a result of Defendants' unlawful and unfair business practices, having lost control over information that has a specific inherent monetary value that can be sold, bartered, or exchanged and the failure to receive any statutory damages to which she may be entitled. She also spent months attempting to address this issue with no compensation for the over 50 hours of time and effort she had to expend as a result of being a victim of these acts of unfair competition, in addition to the increased likelihood of: (i) actual identity theft or compromise; (ii) the loss of the opportunity how their Personal and Medical Information is used; (iii) the compromise, publication, and theft of Personal and Medical Information; (iv) time and expenses associated with the prevention, detection, and recovery from identity theft, and unauthorized use of their Personal and Medical Information; (v) 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; (vi) costs associated with or continuing to have in place freezes or monitoring on credit reports; (vii) the continued risk to Personal and Medical Information, 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 Personal and Medical Information of current and former students and employees and their beneficiaries and dependents; and (viii) 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 Personal

and Medical Information compromised as a result of the cyberattack.

169. Plaintiff and Class members may have no other adequate remedy of law in that, absent injunctive relief from the Court, Defendants are likely to not fully redress the issues raised by their illegal and unfair business practices. Defendants have not announced any specific changes to their data security infrastructure, processes, or procedures to fix the vulnerabilities in the electronic information security systems and security practices that permitted the resulting data breach to occur and go undetected, and thereby prevent further attacks, nor have they provided prompt notice of the circumstances surrounding this breach as required by law.

170. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiff seeks an order of this Court for herself, Class members, and for the benefit of the public granting injunctive relief in the form of requiring Defendants to ensure that SUHSD corrects its illegal conduct, sending out notices that do not reveal student information or otherwise correct and amplify on their previous inadequate notices, to prevent Defendants from not ensuring that SUHSD puts in systems that would prevent the repeat of the illegal and wrongful practices as alleged above and protect and preserve confidentiality of Personal and Medical Information in Defendants' possession that has been accessed, downloaded, exfiltrated, stolen, and viewed by at least one unauthorized third party because of Defendants' illegal and wrongful practices set forth above. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiff also seeks an order of this Court for equitable and injunctive relief in the form of prohibiting Defendants from continuing to refuse publicly issuing comprehensive direct and corrective notices as well as restitution and restitutionary disgorgement of the monies Defendants saved in not having appropriate protective measures in place.

171. This action, if successful, will enforce an important right affecting the public interest and would confer a significant benefit, whether pecuniary or non-pecuniary, for a large class of persons and the general public. Private enforcement is necessary and places a disproportionate financial burden on Plaintiff in relation to Plaintiff's stake in the matter. Because this case is brought to enforce important rights affecting the public interest, Plaintiff also seeks the recovery of attorneys' fees and costs in prosecuting this action against Defendants under Cal. Code Civ. Proc. § 1021.5 and other applicable law.

NINTH CAUSE OF ACTION

DECLARATORY RELIEF

172. Plaintiff incorporates the foregoing allegations by reference as if fully set forth herein to the extent relevant to this Cause of Action and the relief available thereunder.

173. A present and actual controversy exists between the parties. Defendants have failed to acknowledge the wrongful nature of their actions, have not sent affected individuals 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 SUHSD would correct or enact adequate security policies and procedures to protect and preserve Plaintiff's and the Class members' Personal and Medical Information in Defendants' possession.

174. Now that Defendants' insufficient information security is known to hackers, the Personal and Medical Information in Defendants' possession is even more vulnerable to cyberattack and is not less but more likely to take place.

175. Plaintiff and the 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.

176. As described above, Defendants' actions have caused harm to Plaintiff and Class members. Further, Plaintiff and Class members are at risk of additional or further harm due to the exposure of their Personal and Medical Information and Defendants' failure to fully address the security failings that lead to such exposure and provide adequate notice thereof.

177. Plaintiff and Class members seek an order of this Court for declaratory, equitable, and injunctive relief in the form of an order finding Defendants have failed and continue to fail to adequately protect Plaintiff's and the Class members' Personal and Medical Information from release to unknown and unauthorized third parties, requiring Defendants to correct or enact adequate privacy notices they mailed and issued, implement security measures to protect and preserve Plaintiff's and Class members' Personal and Medical Information in its possession, and requiring Defendants to publicly issue comprehensive corrective notices to Plaintiff, Class members and the public.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, both individually and on behalf of the Class and for the benefit of the public, prays for orders and judgment in favor of Plaintiff and the Class and against Defendants as follows, as may be applicable to the Causes of Action set forth above, but not for damages at this time:

A. Finding that this action satisfies the prerequisites for maintenance as a class action under Cal. Code Civ. Proc. § 382 and certifying the Class defined herein;

B. Designating Plaintiff as representative of the Class and her counsel as Class counsel;

C. Declaring Defendants' conduct in violation of the laws set forth above, including Cal. Civ. Code §§ 56.10(a), 56.101, 1798.21, 1798.29, Cal. Bus. and Prof. Code §§ 17200 and 22584 *et seq.*, and Article I, § 1 of the California Constitution.

D. An order:

1. prohibiting Defendants from ensuring that SUHSD stop 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 and that ask them to destroy notices that illegally revealed student information, and publicly issue comprehensive corrective notices to Plaintiff, Class members, and the public;

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 Personal and Medical Information of Plaintiff 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 SUHSD will segment data by, among other things, 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 personal identifying information of Plaintiff and Class members and 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 inform 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

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 Plaintiff's counsel reasonable attorneys' fees and non-taxable expenses;

G. Awarding Plaintiff's costs;

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

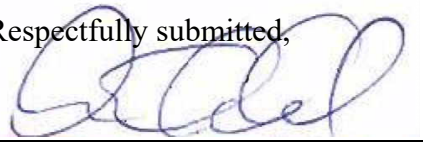
I. Granting such further relief as the Court deems just.

JURY DEMANDED

Plaintiff demands a trial by jury on all issues so triable.

Dated: July 9, 2023

Respectfully submitted,



WHATLEY KALLAS, LLP
Alan M. Mansfield, SBN: 125998
amansfield@whatleykallas.com
16870 W. Bernardo Drive, Suite 400
San Diego, CA 92127
Phone: (619) 308-5034
Fax: (888) 341-5048

APRIL M. STRAUSS, A PC
April M. Strauss, SBN: 163327
astrauss@sfaclp.com
2500 Hospital Drive, Bldg. 3
Mountain View, CA 94040
Phone: (650) 281-7081

DOYLE APC
William J. Doyle II, SBN: 188069
bill@doyleapc.com
Christopher W. Cantrell, SBN: 290874
chris@doyleapc.com
550 West B Street, 4th Floor
San Diego, CA 92101
Phone: (619) 736-0000
Fax: (619) 736-1111

Attorneys for Plaintiff