MDSM
CRAIG J. MARIAM, ESQ.
Nevada Bar No.: 10926
RACHEL L. WISE, ESQ.
Nevada Bar No.: 12303
300 So. 4th Street, Suite 1550
Las Vegas, Nevada 89101
GORDON REES SCULLY MANSUKHANI, LLP
Telephone: (702) 577-9300
Direct: (702) 577-9316
Facsimile: (702) 255-2858
E-Mail: cmariam@grsm.com
rwise@grsm.com

Attorneys for Defendant
Clark County School District

EIGHTH JUDICIAL DISTRICT COURT

CLARK COUNTY, NEVADA

JANE DOE, on behalf of her minor child JOHN DOE and all others similarly situated; and ERIN TIMRAWI, on behalf of herself and all others similarly situated, Plaintiff, vs. CLARK COUNTY SCHOOL DISTRICT, a political subdivision of the State of Nevada; DOES 1 through 10, inclusive; and ROE ENTITIES 1 through X, inclusive, Defendants.	Case No.: A-23-880643-C Dept. No.: 6 **HEARING REQUESTED** **CLARK COUNTY SCHOOL DISTRICT'S MOTION TO DISMISS PLAINTIFFS' COMPLAINT**

Defendants Clark County School District ("CCSD"), by and through its attorneys of the law firm of Gordon Rees Scully Mansukhani, LLP, and pursuant to Nevada Rules of Civil Procedure ("Rule") 12(b)(1) and 12(b)(5), hereby submit this Motion to Dismiss Plaintiffs Jane Doe's and Erin Timrawi's ("Plaintiffs") Complaint in its entirety (the "Motion").

/ / /

/ / /

This Motion is based on the pleadings and papers filed in this action, the attached Memorandum of Points and Authorities, and any oral argument the Court may require at the hearing on the Motion.

Dated: January 31, 2024

Respectfully submitted,

GORDON REES SCULLY MANSUKHANI, LLP

/s/ Rachel L. Wise
Craig J. Mariam, Esq.
Nevada Bar No.: 10926
Rachel L. Wise, Esq.
Nevada Bar No. 12303
300 South Fourth Street, Suite 1550
Las Vegas, Nevada 89101

Attorneys for Defendant
Clark County School District

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

In October of 2023, the Clark County School District ("CCSD") was the victim of a cyber-attack by an unknown third-party Threat Actor (the "Data Security Incident"). CCSD immediately took efforts to respond to the Data Security Incident, including engaging with outside counsel and third party forensic vendors to investigate the scope and nature of the Data Security Incident. In an abundance of caution, CCSD made a public announcement of the Data Security Incident, and in the weeks thereafter continued to provide public updates, including the fact that, in the event sensitive information was impacted in the Data Security Incident, written notice to those impacted by the Data Security Incident would be provided. *See* Compl. at ¶¶ 32 – 37.

Rather than waiting to see if the individuals they purport to represent were actually impacted by the Data Security Incident, Plaintiffs instead ran to the Courthouse only weeks after the Data Security Incident occurred and filed this Complaint. This premature filing resulted in

the inadequate Complaint before the Court, deficient for all the reasons set forth below; but especially lacking given that Plaintiffs have not, and cannot, allege anything more than conclusory and theoretical harm related to the Data Security Incident. Indeed, nowhere in the Complaint is there any non-conclusory allegation that Plaintiffs were *actually impacted* by the Data Security Incident and, indeed, the only non-*Doe* Plaintiff, Erin Timrawi, was not a recipient of the December 28, 2023 Notice regarding the Data Security Incident.[1] The lack of concrete, non-speculative harm alleged by Plaintiffs, on account of their haste to file instead of waiting for factual verification they were actually affected, proves fatal to the Complaint on standing grounds. Further, each of Plaintiffs' eight causes of action fail to properly or sufficiently state a claim upon which relief can be granted. Finally, Plaintiffs' claims are based on discretionary conduct and the existence of a "hazard" in the form of a data security risk that make CCSD immune from liability pursuant to NRS 41.032 and NRS 41.033. Accordingly, the Complaint should be dismissed in its entirety.

II. FACTUAL ALLEGATIONS

On October 5, 2023, CCSD fell victim to a cyber-attack, which was caused by an unknown Threat Actor. Compl., at ¶ 31. On October 16, 2023, CCSD published an announcement notifying individuals that the cyber-attack occurred, that a forensic expert team was retained to investigate the Data Security Incident, and that it was working alongside law enforcement to determine the scope of the attack and that it would be providing Notice to impacted individuals. Compl., at ¶ 32. Plaintiffs allege the following eight claims for relief: (1) Violation of NRS 41.600, (2) Violation of the Nevada Deceptive Trade Practices Act, NRS 598.0901, (3) Negligence and Negligence *Per Se*, (4) Breach of Confidence, (5) Breach of

[1] Defendant is unaware of the Plaintiffs successfully petitioning the Court for the ability to file this action under the "Jane Doe" and "John Doe" pseudonyms. *See generally, Tan v. Eighth Jud. Dist. Ct. in & for Cnty. of Clark*, 516 P.3d 683 (Nev. App. 2022) *citing Does v. Advanced Textile Corp.*, 214 F.3d 1058, 1068-69 (9th Cir. 2000) (providing that a plaintiff may bring suit under a pseudonym where necessary to protect the safety of a person or protect the person from harassment, injury, ridicule, or personal embarrassment so long as the need for anonymity outweighs any prejudice to the opposing party and the public's interest in knowing the party's identity, and further emphasizing that courts should evaluate the need for anonymity during every phase of the proceeding).

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

Fiduciary Duty, (6) Breach of Implied Contract, (7) Unjust Enrichment, and (8) Declaratory Relief. Although they had no notice of the number of individuals or data impacted, Plaintiffs speculate that the Personally Identifiable Information ("PII") or Protected Health Information ("PHI") (collectively, "Sensitive Information") of individuals was impacted. Compl. at ¶ 33.

III. LEGAL ANALYSIS

A. Plaintiffs Have Not Alleged a Sufficient Injury-in-Fact Necessary to Establish Standing to Bring this Action.

"Nevada has a long history of requiring an actual justiciable controversy as a predicate to judicial relief." *Israyelyan v. Chavez*, 136 Nev. 832, 466 P.3d 939 (2020) (internal quotation omitted). Thus, to pursue a legal claim, an "injury in fact" must exist. The "injury-in-fact" analysis requires the claimant to show that the action caused or threatened to cause the claimant's injury-in-fact, and that the relief sought will remedy the injury. *Id., citing Bennett v. Spear*, 520 U.S. 154, 167 (1997). Further, "standing requires that a plaintiff have suffered an 'injury in fact' that is not merely conjectural or hypothetical" and there must "be a causal connection between the injury and the conduct complained of." *Miller v. Ignacio*, 112 Nev. 930, 936, 921 P.2d 882, 885 (1996).

Here, Plaintiffs have alleged no concrete injury in fact that is sufficient to establish standing. All of their alleged categories of harm are nothing but speculative in nature. *See e.g.* Compl. at ¶ 76 (alleging only hypothetical or theoretical damages such as: the loss of the opportunity to control how their PII is used; the potential compromise, publication, and theft of their PII; time and expenses associated with the prevention, detection, and recovery from theoretical identity theft, tax fraud, and unauthorized use of their PII; lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate consequences of the Data Security Incident; general undefined continued risk to Plaintiffs' PII; and future costs in terms of time, effort, and money that will be spent to prevent, detect, contest, and repair the theoretical impact of the Data Security Incident on Plaintiffs' PII). Further, given the Plaintiffs rushed to file this Complaint before seeing if they were even impacted by the Data Security Incident, the Complaint is devoid of allegations sufficient to

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

demonstrate a causal connection between these alleged "injuries" and that Data Security Incident. The lack of *any factual allegations* about any of the Named Plaintiffs' information actually being affected in the Data Security Incident is fatal to Plaintiffs' claims.[2] Accordingly, Plaintiffs' Complaint should be dismissed on account of a lack of standing to bring this action.

B. Plaintiffs' Claims Should be Dismissed for Failure to State Claims Upon Which Relief can be Granted.

Pursuant to NRCP 12(b)(5), a motion to dismiss is properly granted where the allegations in the complaint, "taken at face value . . . and construed favorably in the [plaintiff's] behalf, fail to state a cognizable claim for relief." *Morris v. Bank of Am. of Nev.*, 110 Nev. 1274, 1276, 886 P.2d 454, 456 (1994) (citations omitted). While this Court must presume the truth of the factual allegations, it is not required to "necessarily assume the truth of legal conclusions merely because they are cast in the form of factual allegations in [the] Complaint." *McMillan v. Dep't of Interior*, 907 F.Supp. 322, 327 (D. Nev. 1995). Moreover, pleading of conclusions must be "sufficiently definite to give fair notice of the nature and basis or grounds of the claim and a general indication of the type of litigation involved." *Taylor v. State of Nevada*, 73 Nev. 151, 311 P.2d 733 (1957). Additionally, "the court may take into account matters of public record, orders, items present in the record of the case, and any exhibits attached to the complaint when ruling on a motion to dismiss for failure to state a claim upon which relief can be granted." *Breliant v. Preferred Equities Corp.*, 109 Nev. 842, 848 P.2d 1258 (Nev. 1993). Finally, a 12(b)(5) motion must be granted if the district court determines "that the Plaintiff could prove no set of facts which, if accepted by trier of fact, would entitle him or her to relief." *Simpson v. Mars, Inc.*, 113 Nev. 188, 929 P.2d 966 (1997); *see also, Bergmann v. Boyce*, 109 Nev. 670, 856 P.2d 560 (1993).

1. Plaintiffs Failure to Sufficiently Allege Damages is Fatal to their Statutory Claims (Counts I & II), their Negligence Claim (Count III), their Breach of Confidence Claim (Count IV); their Breach of Implied Contract Claim (Count VI) and their Unjust Enrichment Claim (Count VII).

[2] Indeed, the only non-Doe Plaintiff, Erin Timrawi, was not one of the individuals who was a recipient of the Notice of the Data Security Incident sent out on December 28, 2023.

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

This case is analogous to a recent 2022 decision by the District of Nevada dealing with a Data Breach and Nevada-based claims very similar to those causes of action alleged by Plaintiffs in this case. In *Pruchnicki v. Envision Healthcare Corp*., plaintiffs alleged claims for negligence, breach of implied contract, negligent misrepresentation, and violation of Nevada Revised Statute ("NRS") § 41.600 in connection with a healthcare data breach. *See* 439 F. Supp. 3d 1226, 1229 (D. Nev. 2020), aff'd, 845 F. App'x 613 (9th Cir. 2021). In granting the defendant's motion to dismiss, the District Court found that plaintiffs' allegations of harm "in the form of lost time mitigating the effects of the data breach, emotional distress, the imminent and certainly impending injury flowing from potential fraud and identity theft, diminution in value of her personal and financial information, and continued risk to her personal data" were insufficient to constitute allegations of damages necessary for any of her claims to survive beyond the pleading stage. *Id*. at 1236 (intentional citations omitted)[3]; *see also Gardiner v. Walmart Inc.*, 2021 WL 2520103 at *7 (N.D.CA 2021) (dismissing a data breach class action because "Plaintiff's vague and conclusory allegations regarding his purported injuries are insufficient to establish the damages element required for his breach of contract, negligence, and UCL claims."); *Holly v. Alta Newport Hospital, Inc.*, 612 F.Supp.3d 1017, 1027 (C.D. Cal. 2020) ("finding plaintiff's 'conclusory and vague allegations insufficient to establish that she suffered actual damages as a result of the data breach"); *Razuki v. Caliber Home Loans, Inc.*, 2018 WL 6018361 at *1 (S.D. Cal. 2018) (plaintiff's allegations "too conclusory and vague to satisfy the pleading standard in a complex, large-scale, data breach class action"); *Ruiz v. Gap, Inc.*, 622 F.Supp.2d 908, 916 (N.D. Cal. 2009) (granting summary judgment for failure to show cognizable harm despite "fear of future identity theft"), aff'd, 380 F. App'x 689, 693 (9th Cir. 2010). Plaintiffs in this case have alleged essentially the same exact categories of speculative damages as in the *Pruchnicki* case, and this Court should adopt the reasoning of that Court in finding that Plaintiffs have not sufficiently pled the damages elements of these claims.

[3] As to allegations of emotional distress, dispositive to the *Pruchnicki* court was the Nevada requirement of allegations of a physical-manifestation for such harms to be recoverable. *See*, 439 F. Supp. at 1234. As in *Pruchnicki*, Plaintiffs in this case have not alleged any necessary physical manifestation of their alleged emotional distress.

2. Plaintiffs' Statutory Claims Are Factually Deficient.

As addressed above, Plaintiffs' claims pursuant to the Nevada Consumer Fraud Act ("NCFA") and the Nevada Deceptive Trade Practices Act ("NDTPA") fail because Plaintiffs have not alleged a cognizable injury caused by the Data Security Incident. They also fail given that Plaintiffs have not plead these claims with the particularity required by NRCP 9(b).

Plaintiffs NCFA Claim (Count I), and NDTPA Claim (Count II) are based on allegations of "consumer fraud" or "deception" Compl. at ¶¶ 87 – 111. Accordingly, Plaintiffs must plead these claims with particularity rather than alleging only general violations of these statutes. *See Brown v. Keller*, 97 Nev. 582, 583 (1981) (requiring Plaintiff to identify the time, place, and circumstances of the defendant's alleged conduct in their complaint to comply with heightened pleading standard in NRCP 9(b)). Here, Plaintiffs alleged violations of these statutes are vague, speculative, and conclusory and fail to include the time, place and detailed circumstances of any violation. While Plaintiffs allege, "CCSD failed to comply with [alleged applicable standards]," thereafter, Plaintiffs provide only generic and conclusory allegations of what CCSD failed to do in order to protect Plaintiffs' PII. Compl. at ¶ 96. Such "conclusory allegations of wrongdoing that are too vague to state a valid claim for fraud under the heightened pleadings standards." *Mauer v. Am. Home Mortg. Acceptance, Inc.*, 2011 WL 6752631, at *4 (D. Nev. 2011).

When alleging a NDTPA claim in particular, generally a Plaintiff must allege some knowing false representation, or some express failure to "disclose a material fact." *See Teva Parenteral Medicines, Inc. v. Eighth Judicial District Court in and for Court of Clar*k, 137, Nev 51, 62, 481 P.3d 1232, 1241 (2021). Here, Plaintiffs' Complaint is deficient because it contains neither allegations of any knowingly false representation, nor any non-conclusory allegations of purposeful omissions. Indeed, Plaintiffs do not allege any express promises made by CCSD regarding data security practices, they do not explain with particularity how CCSD failed to employ data security practices, they do not allege facts showing CCSD knew it failed to employ such data security practices, they do not identify the precise disclosures CCSD should have made regarding any data security practices, and they do not allege how such disclosures should have

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

been presented to Plaintiffs. Compl. at ¶ 96. Without the specificity required by NRCP 9(b), Counts I and II are facially deficient, and the claims must be dismissed.

3. Plaintiffs' Negligence and Negligence Per Se Claims Are Insufficiently Pled.

"[T]o prevail on a standard negligence claim, a plaintiff must establish four elements: (1) the existence of a duty of care, (2) breach of that duty of care, (3) legal causation, and (4) damages." *Sanchez ex rel. Sanchez v. Wal-Mart Stores, Inc.*, 125 Nev. 818, 824 (2009). As to a negligence *per se* theory, "a violation of [a] statute establishes the duty and breach elements of negligence only if the injured party belongs to the class of persons that the statute was intended to protect, and the injury is of the type against which the statute was intended to protect." *Ashwood v. Clark Cnty.*, 113 Nev. 80, 86, 930 P.2d 740, 744 (1997). Here, Plaintiffs fail to properly allege the damages and causation elements required by a standard negligence claim or one brought pursuant to a negligence *per se* theory, both as to the Data Security Incident itself and as to any "delay" in the Notice regarding the Data Security Incident.

First, for all the reasons discussed in Sections III(A) and III(B)(1) above, Plaintiffs have not sufficiently alleged damages or causation related to the Data Security Incident itself. Further, "[t]o allege a 'cognizable injury' arising from delay [in the data breach context], a plaintiff must allege 'incremental harm suffered as a result of the alleged delay in notification,' not merely the data breach itself." *Stallone v. Farmers Group, Inc.*, 2022 WL 10091489, at *8 (D. Nev. 2022) *quoting Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *6 (S.D. Cal. 2016). Here, Plaintiffs do allege "harm" based on a delay in notice regarding the Data Security Incident, however, instead of pleading incremental damages, Plaintiffs simply restate the same damages that they allegedly suffered as a result of the data breach. *See e.g.* Compl., at ¶ 76. Finally, given the fact that Plaintiffs filed this Complaint before receiving any indication that they were *actually impacted* by the Data Security Incident, Plaintiffs have not, and cannot, sufficiently allege the causation element of this claim.

Second, Plaintiffs' negligence claims cannot survive the economic loss rule, which bars recovery in tort absent personal injury or property damage. *Nev. Power Co. v. Trench France,*

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

S.A.S., 2020 WL 6689340, at *4 (D. Nev. 2020) ("The economic-loss doctrine is the judicially created rule that cabins the ability to recover purely monetary damages to contract-based theories, barring recovery in tort."); *Terracon Consultants W., Inc. v. Mandalay Resort Grp.*, 125 Nev. 66, 73 (2009) (economic loss rule "bars unintentional tort actions when the plaintiff seeks to recover 'purely economic losses'"); *Bustos v. Dennis*, 2020 WL 5763603, at *4 (D. Nev. 2020) ("Here, Bustos alleges that he lost commissions and service fees that he speculates would have been earned by his distribution network of agents. This is exactly the type of damages alleged by the plaintiff in *Desert Salon* which the court found to be 'purely economic losses' barred by the economic loss doctrine."). Plaintiffs allege no personal injury or property damage. Accordingly, the economic loss rule bars their negligence claims.

Third, Plaintiffs' negligence *per se* theory fails because none of the statutes or regulations, state or federal, that Plaintiffs allege as the basis for this claim provide Plaintiffs with a private cause of action. See Compl. at ¶ 116 (alleging violations of state statures NRS 598.0903 *et seq;* NRS 603A.210 & .220, NRS 392.029, and NAC 388.289; federal statues including the FTC Act, FERPA, and various HIPAA subparts; CCSD Policies 5125 & 5138; and CCSD Regulations 1212, 4311, and 5125.1). Indeed, the Nevada Supreme Court has held that when a governmental duty runs to the public generally (as many of the obligations created pursuant to these statutes do), no private cause of action is created by a breach of such duty. *See Whalen v. County of Clark*, 96 Nev. 559, 613 P.2d 407 (1980); *Bruttomesso v. Las Vegas Met. Police*, 95 Nev. 151, 591 P.2d 254 (1979). This Court should join other courts in the data breach context who have dismissed similar negligence *per se* claims based on statutes that did not provide an independent cause of action. *See e.g., In re: Netgain Tech., LLC*, No. 21-CV-1210 (SRN/LIB), 2022 WL 1810606, at *16 (D. Minn. June 2, 2022) (dismissing negligence per se cause of action because the FTC does not grant a private right of action and finding no precedent in California, Minnesota, Nevada, South Carolina, or Wisconsin that would permit state law negligence per se claims to proceed under theory of violation of Section 5 of FTC Act); *Levy-Tatum v. Navient Sols., Inc.*, 183 F. Supp. 3d 701, 707 (E.D. Pa. 2016) (internal citation omitted) ("the absence of a private right of action in a statutory scheme is an indicator that the statute did

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

not contemplate private enforcement"); *Jupiter Inlet Corp. v. Brocard*, 546 So.2d 1, 2–3 (Fla. Dist. Ct. App. 1998)) (refusing to recognize a private right of action for negligence per se based on an alleged violation of a federal statute that does not provide for a private right of action); *Walters v. Blue Cross & Blue Shield of Texas, Inc.*, No. 3:21-CV-981-L, 2022 WL 902735, at *6 (N.D. Tex. Mar. 28, 2022) (finding that the Health Insurance Portability & Accountability Act ("HIPAA") and the Texas Medical Records Privacy Act cannot form basis for negligence per se claim because statutes do not contain private right of action and "to hold otherwise would run afoul of legislative intent.").

4. Plaintiffs Have Failed to Plead the Intent Necessary to State a Claim for Breach of Confidence.[4]

Generally, to state a claim for breach of confidence, a plaintiff must allege that a person knowingly disclosed nonpublic information that the defendant learned within a confidential or special relationship. *See e.g. Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 932 (11th Cir. 2020); *Kamal v. J. Crew Grp., Inc.*, 918 F.3d 102, 114 (3d Cir. 2019); *Fernandez-Wells v. Beauvais*, 983 P.2d 1006, 1009 (N.M. 1999); *Enter Research Group, Inc. v. Genesis Creative Group, Inc.*, 122 F.3d 1211, 1226-27 (9th Cir. 1997) (construing California law). Indeed, in many cases in the data breach context Courts have dismissed claims for breach of confidence based on allegations of insufficient security practices leading to the disclosure of Sensitive Information. *See e.g. Farmer v. Humana, Inc.,* 582 F. Supp.3d 1176, 1189 (M.D. Flo. 2022) (a breach of confidence claim does not lie where a defendant's inadequate security facilitated the theft of information by third-parties); *Muransky*, 979 F.3d at 932 (same); *Purvis v. Aveanna Healthcare LLC*, 563 F. Supp. 3d 1360, 1377 (N.D. Ga. 2021) (same).

[4] The Defendant is not aware of Nevada case law directly addressing this claim, which is why it is very likely that it is not a recognized cause of action in the state, as is the case in many other jurisdictions. *See e.g., Mucklow v. John Marshall L. Sch.*, 531 N.E.2d 941, 946 (Ill. App. 1988) (refusing to extend common law tort of breach of confidence beyond trade secret context under Illinois law); *Viscuso v. Quicken Loans, Inc.*, No. 3:21-CV-01924-JMC, 2022 WL 845859, at *4 (D.S.C. Mar. 22, 2022) (refusing to extend tort of breach of confidentiality in data breach class action to cases against non-physicians under South Carolina law); *In re Capital One*, 488 F. Supp. 3d at 409 n.21 (dismissing breach of confidence causes of action as invalid under Texas and Virginia state law); *Raiser v. The Church of Jesus Christ of Latter-Day Saints*, No. 2:04-CV-896, 2006 WL 288442, at *9 (D. Utah Feb. 7, 2006) (questioning plaintiff's assumption that breach of confidence exists as viable cause of action in Utah).

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

Here, Plaintiffs have not pled sufficient facts showing that CCSD knowingly *disclosed* Plaintiffs' PII, as Plaintiffs acknowledge throughout their Complaint that the breach was perpetrated by cyber criminals and that the information was *stolen* and access to it was unauthorized by CCSD. *See e.g.* Compl. ¶ 1, 31, 32, & 137. Accordingly, the claim for breach of confidence, to the extent it is even recognized in Nevada, should be dismissed.

5. Plaintiffs' Do Not Sufficiently Allege the Existence of a Fiduciary Relationship Between the Parties, so their Claim for Breach of Fiduciary Duty Must be Dismissed.

"[A] breach of fiduciary duty claim seeks damages for injuries that result from the tortious conduct of one who owes a duty to another by virtue of the fiduciary relationship." *Stalk v. Mushkin*, 125 Nev. 21, 28 (2009). "There are three elements in a claim for breach of fiduciary duty: (1) the existence of a fiduciary duty; (2) breach of that duty; and (3) the breach proximately caused the damages." *Id*. "[T]raditional examples of fiduciary relationships include those of trustee/beneficiary, corporate directors and majority shareholders, business partners, joint adventurers, and agent/principal." *Gilman v. Dalby*, 176 Cal. App. 4th 606, 613 (2009). "Inherent in each of these relationships is the duty of undivided loyalty the fiduciary owes to its beneficiary, imposing on the fiduciary obligations far more stringent than those required of ordinary contractors." *Id.*

In other jurisdictions, "courts have routinely rejected a 'guardian of personal information' theory as a basis for imposing fiduciary duty." *In re Premera Blue Cross Customer Data Security Breach Litigation*, 198 F.Supp.3d 1183, 1201 (D.D. Oregon, 2016) *quoting Cooney v. Chicago Public Schools*, 407 Ill.App.3d 358 (2010). In *Premera*, the Court found that plaintiffs did not allege that they were "induced to relax the care and vigilance that they otherwise should, and ordinarily would exercise concerning their confidential information." *Id*. The Court rejected the plaintiffs' argument that was if they had "known how Premera actually would be treating their Sensitive Information, they would not have entered into any relationship with Premera," in dismissing their breach of fiduciary duty claim. *Id*. *See also, e.g., In re Ambry Genetics Data Breach Litigation*, 567 F.Supp.3d 1130, 1144-5 (D.C.D. Cal., 2021) (dismissing plaintiffs' cause of action for breach of fiduciary duty because simply alleging that defendants collected

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

plaintiffs' private information so defendants could provide genetic testing to screen for and diagnose diseases was not a situation where the parties had a special relationship); *In re Mednx Services, Inc., Customer Data Security Breach Litigation*, 603 F.Supp.3d 1183, 1226 (D.S.D. Fla., 2022) (dismissing plaintiffs' cause of action for breach of fiduciary duty because "blandly assert[ing] that Defendants owed them a duty of confidentiality 'because [they] entrusted their sensitive personal information to Defendants in exchange for receiving services.'").

Here, Plaintiffs have failed to allege how the named Plaintiffs are in a fiduciary relationship with CCSD. Instead, they just allege generally that CCSD was in receipt of Plaintiffs Sensitive Information. *See* Compl. at ¶ 145 ("Defendants' acceptance and storage of Plaintiffs' and Class members' PII, as well as for Plaintiffs' and many members of the Class, their status as employees and students of CCSD, created a fiduciary relationship between Defendants, on the one hand, and Plaintiffs and Class members on the other hand. In light of this relationship, Defendants must act primarily for the benefit of such persons, which includes safeguarding and protecting Plaintiffs' and Class members' PII."). This argument that receipt of personal information creates a fiduciary duty is the same argument which has been routinely rejected by other courts, as discussed above. Accordingly, this claim should be dismissed.

6. Plaintiffs' Implied Contract Claim Lacks Factual Allegations Supporting the Existence of an Enforceable Contract Between Plaintiffs and CCSD.

To state a claim for breach of an implied contract, as with an express contract, Plaintiffs must show: "(1) the existence of a valid contract; (2) a breach by the defendant; and (3) damage as a result of the breach." *Mizrahi v. Wells Fargo Home Mortg.*, 2010 WL 2521742, at *3 (D. Nev. 2010). Further, contracts require a mutual assent or a "meeting of the minds" by both parties as to "the contract's essential terms." *Grisham v. Grisham*, 128 Nev. 679, 685, 289 P.3d 230, 235 (2012).

Here, Plaintiffs' breach of implied contract claim fails because it does not sufficiently plead any facts establishing a meeting of the minds between CCSD and Plaintiffs to enter into any "agreement" alleged in the Complaint. The implied "contracts" are not described with any specificity, and Plaintiffs instead only claim in a conclusory fashion that they, "provided their PII

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

to Defendant in exchange for employment or the provision of educational or medical services, along with Defendants' promise to protect their PII from unauthorized disclosure." Compl. at ¶ 151. Numerous courts have rejected implied contract theories in the data breach context where, as here, Plaintiffs do "not allege that [CCSD] affirmatively promised that [Plaintiffs] data would not be hacked." *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 717 (8th Cir. 2017); *see also e.g. Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010) (dismissing implied contract claim because factual allegations failed to demonstrate a meeting of the minds of any specific offer to encrypt or otherwise safeguard plaintiffs' personal data); *Frezza v. Google Inc.*, No. 12-CV-00237-RMW, 2012 WL 5877587, at *4 (N.D. Cal. Nov. 20, 2012) (dismissing implied contract claim and explaining that "even if an implied contract does indeed exist, plaintiffs must sufficiently plead that Google agreed to and then breached a specific obligation"); *Antman v. Uber Techs., Inc.*, 2018 WL 2151231, at *12 (N.D. Cal. 2018) ("[P]laintiffs have not plausibly pleaded a claim for breach of an implied contract. . . . They plead no facts about the existence of an implied contract, such as mutual assent and the other elements necessary to establish an express contract").

Further, the uncertainty about the "terms" of any implied contract here make Plaintiffs allegations regarding breach insufficient. *See Grisham*, 128 Nev. at 685. ("A valid contract cannot exist when material terms are lacking or are insufficiently certain and definite for a court to ascertain what is required of the respective parties and to compel compliance if necessary.") (Internal citations omitted). Plaintiffs do not allege that the implied contract required perfect data security such that no breach could ever occur. Rather, Plaintiffs claim, "[CCSD] breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII, which was compromised as a result of the data breach issue herein." Compl. at ¶ 157. Plaintiffs do not allege how CCSD violated this alleged promise other than the fact that the Data Security Incident occurred. As courts have recognized, the claim that CCSD "fail[ed] to [implement] reasonably safeguard[s]" "does not assert more than the mere possibility of misconduct." *Kuhns*, 868 F.3d at 717. Indeed, the "implied premise that because data was hacked [CCSD]'s protections must have been inadequate is a naked

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

assertion[ ] devoid of further factual enhancement that cannot survive a motion to dismiss." *Id.* (citations omitted). Beyond that "naked assertions," Plaintiffs' "vague allegations do not establish how [CCSD] failed to take reasonable measures to protect [Plaintiffs'] data." *Gardiner*, 2021 WL 2520103 at *6; *see also Razuki*, 2018 WL 2761818, at *3.

Finally, this claim is also deficient due to a lack of sufficiently pled damages as discussed in Section III(B)(1) above. Accordingly, Plaintiffs' breach of implied contract cause of action must be dismissed.

7. Plaintiffs Have Failed to State a Claim for Unjust Enrichment.

To state an unjust enrichment claim, Plaintiffs must show: "(1) a benefit conferred on the defendant by the plaintiff; (2) appreciation of the benefit by the defendant; and (3) acceptance and retention of the benefit by the defendant (4) in circumstances where it would be inequitable to retain the benefit without payment." *Ames v. Caesars Ent. Corp.*, 2019 WL 1441613, at *5 (D. Nev. 2019). Here, Plaintiffs fail to allege that they "bestow[ed] . . . any gratuitous benefit upon" CCSD. *See In re Zappos*, 2013 WL 4830497, at *5 (applying Nevada law). An unjust enrichment claim "means more than that the defendant has profited unscrupulously while the plaintiff has been harmed." *Id.* The claim "only lies against a defendant who has willingly received the plaintiff's labor or goods without giving anything of equal value in return under circumstances where it would be inequitable not to require payment or 'restitution' therefore." *Id*. Plaintiffs allege no such facts here. Instead, they allege in a conclusory fashion that CCSD benefitted simply by receiving and using Plaintiffs' and Class members' PII, which they allege was somehow used for CCSD's own benefit when the reality is, at least as to CCSD students, those *students* received the benefit of a public education. Accordingly, Plaintiffs' cause of action for unjust enrichment is insufficiently pled, and this court should join other courts throughout the country who have dismissed unjust enrichment claims in the data breach context. *See e.g., Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016) (dismissing unjust enrichment claim where plaintiff "paid for food products. She did not pay for a side order of data security and protection; it was merely incident to her food purchase").

/ / /

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

8. Plaintiffs' Claim for Declaratory Relief is not a Valid Cause of Action.

"Declaratory relief, like injunctive relief, is a remedy, not an underlying substantive claim." *Gaming*, 2016 WL 5799300 (D. Nev., 2016) *quoting Daisy Trust*, No. 2:13-cv-00966-RCJ-VCF, 2013 WL 6528467, at *4 (D. Nev., 2013). In dismissing the cause of action, the *Gaming* court found that Plaintiffs allegations "merely repeats the allegations supporting Plaintiff[s'] [earlier] claims. It is therefore duplicative and [should be] dismissed." *Id.* So too is the case here, this claim simply repeats the allegations supporting Plaintiffs' first seven claims and it must be dismissed.

C. CCSD is Immune from Liability Pursuant to NRS 41.032 & NRS 41.033.

At the crux of Plaintiffs' allegations are claims that CCSD was somehow delinquent in the application of data privacy and security measures—all of which are discretionary activities for which CCSD has immunity pursuant to NRS 41.032. "Nevada jurisprudence provides a two-part test for determining whether discretionary-function immunity under NRS 41.032 applies to shield a defendant from liability." *Clark Cnty. Sch. Dist. v. Payo*, 133 Nev. 626, 631, 403 P.3d 1270, 1275–76 (2017). "Under the two-part test, a government defendant is not liable for an allegedly negligent decision if the decision (1) involves an "element of individual judgment or choice," and (2) is "based on considerations of social, economic, or political policy." *Id.* Functionally, Nevada courts have held that for the immunity to apply, it must be both, "discretionary and policy-based." *Id.* Here, all of Plaintiffs' allegations regarding the Data Security Incident relate to discretionary CCSD application, use and adoption of data privacy and cyber security measures, which are based on considerations related to expense and student/employee impact, making them both economic and socially based. *See e.g.,* Compl. at ¶ 4 ("CCSD failed to implement reasonable and adequate security procedures"); ¶ 14 ("[CCSD] fail[ed] to follow applicable, required and appropriate protocols, policies and procedures regarding data access and encryption as well as appropriate procedures, such as two-step or multi-factor authentication"); ¶ 30 ("there is no evidence that CCSD took well-known proactive steps, like requiring multi-factor authentication for all email accounts [and] having robust password protocols . . .).

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

Similarly, CCSD is also immune pursuant to 41.033 which, "was designed to provide governmental agencies immunity for: (1) failing to inspect, whether or not a duty to inspect exists; or (2) failing to discover a hazard, whether or not an inspection is performed." *Chastain v. Clark Cnty. Sch. Dist.*, 109 Nev. 1172, 1175, 866 P.2d 286, 288 (1993). Again, Plaintiffs allegations are all borne out of Plaintiffs' claims that CCSD failed to identify a hazard in the form of a data privacy or cyber security weakness in CCSD electronic systems.

Therefore, Plaintiffs' complaint should be dismissed with prejudice as CCSD is immune from the claims alleged therein.

IV. CONCLUSION

Plaintiffs have not and cannot plead any cognizable damages or harm, proving fatal to their ability to have standing to bring this claim, as well as their ability to sufficiently plead their alleged causes of action. Further CCSD has immunity from the claims in Plaintiffs Complaint. For these reasons, as well as the other deficiencies identified above, Plaintiffs' Complaint should be dismissed in its entirety.

Dated: January 31, 2024

Respectfully submitted,

GORDON REES SCULLY MANSUKHANI, LLP

/s/Rachel L. Wise
Craig J. Mariam, Esq.
Nevada Bar No.: 10926
Rachel L. Wise, Esq.
Nevada Bar No. 12303
300 South Fourth Street, Suite 1550
Las Vegas, Nevada 89101

Attorneys for Defendant
Clark County School District

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on the 31st day of January, 2024, I served a true and correct copy of **CLARK COUNTY SCHOOL DISTRICT'S MOTION TO DISMISS PLAINTIFFS' COMPLAINT** via the Court's Electronic Filing/Service system upon all the parties on the E-Service Master List as follows:

Stephen R. Hackett, Esq.
Johnathon Fayeghi, Esq.
Matthew S. Fox, Esq.
David B. Barney, Esq.
SKLAR WILLIAMS PLLC
410 South Rampart Boulevard, Suite 350
Las Vegas, Nevada 89145
shackett@sklar-law.com
jfayeghi@sklar-law.com
mfox@sklar-law.com
dbarney@sklar-law.com

Attorneys for Plaintiffs

/s/ Gayle Angulo
An Employee of GORDON REES SCULLY MANSUKHANI, LLP

Gordon Rees Scully Mansukhani, LLP
300 S. 4th Street, Suite 1550
Las Vegas, NV 89101