Adam Hosmer-Henner (NSBN 12779)
Chelsea Latino (NSBN 14227)
Jane Susskind (NSBN 15099)
McDONALD CARANO LLP
100 West Liberty Street, Tenth Floor
Reno, Nevada 89501
(775) 788-2000
ahosmerhenner@mcdonaldcarano.com
clatino@mcdonaldcarano.com
jsusskind@mcdonaldcarano.com

LATHAM & WATKINS LLP
Serrin Turner (*Pro Hac Vice*)
1271 Avenue of the Americas
New York, New York 10022
(212) 906-1200
serrin.turner@lw.com

Attorneys for Defendant Caesars Entertainment, Inc.

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

MARK HUDDLESTON, individually and on behalf of all others similarly situated; Plaintiff, v. CAESARS ENTERTAINMENT, INC., Defendant.	Case No. 2:26-cv-01237-APG-EJY CLASS ACTION **DEFENDANT CAESARS ENTERTAINMENT, INC.'S MOTION TO DISMISS AMENDED CLASS ACTION COMPLAINT** **ORAL ARGUMENT REQUESTED**

Defendant Caesars Entertainment, Inc. ("Caesars") hereby moves to dismiss the Amended Class Action Complaint ("Complaint" or "ACAC") (ECF No. 4) filed by Plaintiff Mark Huddleston.

The Complaint should be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(1), because Plaintiff lacks Article III standing to pursue his claims; and pursuant to Federal Rules of Civil Procedure 12(b)(6) and 9(b), because the Complaint fails to state a claim. This motion to dismiss is based upon the following memorandum of points and authorities, together with all accompanying documents and exhibits, and such oral argument or other materials as may be presented in connection with the hearing of this matter.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

RULES

OTHER AUTHORITIES

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiff filed this lawsuit reflexively after learning that Caesars had experienced a cybersecurity incident (the "Incident"), even though he suffered no discernible harm as a result. Instead, Plaintiff tries to punch his ticket to court by reciting the same stock set of "injuries" that appear in virtually every data breach complaint—an "increased risk" of future identity theft, "diminished value" of personal information, and vague allegations about "anxiety" and "loss of privacy"—without plausibly tying them to *this* Incident and the limited data it involved. None of the alleged injuries are sufficient to support Article III standing. And because Plaintiff fails to allege any wrongdoing by Caesars in connection with the Incident, much less damages caused by that conduct, each of Plaintiff's claims is fatally flawed on the merits as well.

Plaintiff lacks Article III standing. Plaintiff—who states only that his "contact information" and date of birth were compromised in the Incident—does not allege any actual injuries that can be attributed to the Incident. Instead, Plaintiff's core theory of harm rests on a supposed "*increased risk* of additional harm from identity theft and identity fraud." ACAC ¶ 99. This theory fails on its face, for two reasons. First, as the Supreme Court unequivocally held in *TransUnion LLC v. Ramirez*, a mere "risk of future harm" cannot supply standing for a damages claim; rather, standing arises only if the risk has actually materialized, and Plaintiff does not allege any actual occurrence of identity theft here, let alone one fairly traceable to the Incident. 594 U.S. 413, 415 (2021). Second, Plaintiff's allegations about facing an increased risk of identity theft are fundamentally implausible here in any event, given that the limited information that was compromised could not plausibly be used by a bad actor to take over Plaintiff's identity. Thus, Plaintiff's boilerplate allegations about the risk of identity theft do not provide a basis for standing. Nor can Plaintiff convert this inadequately pled future risk into an adequately pled present harm, by conclusorily alleging that he feels "anxiety" about the risk, or that he has taken supposed mitigation measures with respect to that risk. Standing requirements would be far too easy to evade if such bootstrapping were sufficient to circumvent them. The Complaint should therefore be dismissed for lack of Article III standing.

/ / /

Plaintiff's claims fail on the merits. Beyond his lack of standing, each of Plaintiff's claims is insufficiently pled. His negligence claim fails because he does not plausibly plead any wrongdoing by Caesars constituting a breach of duty, nor any cognizable tort damages—defects that also doom his implied contract claim. Plaintiff's unjust enrichment claim cannot proceed because it is an equitable claim, and Plaintiff fails to plausibly plead a lack of legal remedies. Finally, Plaintiff's claim under the Nevada Consumer Fraud Act fails on numerous grounds, chief among them that Plaintiff fails to plead any specific misrepresentation or omission of material fact concerning Caesars' data security practices.

In short, the mere fact of a data breach does not provide a free pass to federal court or an entitlement to damages where none exist. Because that mere fact is all the Complaint is ultimately based on, it should be dismissed.

II. BACKGROUND

Caesars is a Nevada-based hospitality and gaming company that, through various subsidiaries, owns and operates hotel, casino, and resort properties throughout the United States. ACAC ¶ 2. Plaintiff Mark Huddleston is a Caesars customer who regularly gambled with Caesars both online and in person. *Id.* ¶ 14. While doing so, Plaintiff alleges that he provided certain personally identifiable information ("PII") to Caesars. *Id.* ¶¶ 14

A. 2026 Data Breach and Plaintiff's Alleged Injuries

In or around March 2026, Caesars experienced a cybersecurity incident in which criminal third parties exfiltrated certain Caesars' customer data. ACAC ¶¶ 43–45. The Complaint alleges virtually no details about the Incident, other than to claim "[u]pon information and belief" that Plaintiff's contact information and date of birth was compromised in the Incident. *Id.* ¶ 45. Plaintiff otherwise alleges that he "remain[s] in the dark" about any other details of the Incident, including "exactly what data was stolen, the particular method of disclosure, the results of any investigations, and what steps are being taken" to remediate the Incident. *Id.* ¶ 50.

Despite what little he professes to know about the Incident, Plaintiff alleges a laundry list of "actual and present injuries" that the Incident supposedly caused. *Id.* ¶ 8. This includes a supposed increased risk of identity theft and fraud; "diminution of the value" of Plaintiff's private information;

lost "benefit of the bargain" damages based on his supposed "overpayment" for services from Caesars; unspecified "out-of-pocket" costs and time spent dealing with the Incident; and increased "anxiety, annoyance, and nuisance." *Id.* ¶ 8. For his part, however, Plaintiff does not allege that he has actually experienced any identity theft, fraud, or out-of-pocket losses due to the Incident, nor does he specify any reasonable mitigation steps he was forced to take in response. Nor does Plaintiff offer any explanation of how the limited information of his that he alleges to have been affected—i.e., his birthdate and contact information—could be used to steal his identity and defraud him. *Id.* ¶ 45.

B. Plaintiff's Complaint and Procedural Background

Plaintiff filed suit on April 22, 2026, on behalf of himself and a putative nationwide class consisting of "[a]ll persons in the United States whose Private Information was compromised in the Caesars' Data Breach discovered in March 2026." ACAC ¶ 102. The Complaint asserts claims for negligence, breach of implied contract, unjust enrichment, and violation of the Nevada Consumer Fraud Act. *Id.* ¶ 10. Plaintiff seeks both damages and injunctive relief relating to Caesars' data security practices. *Id.* at Prayer for Relief.

III. LEGAL STANDARDS

Rule 12(b)(1). The party invoking federal jurisdiction bears the burden of establishing standing. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). To do so, a plaintiff must show an injury in fact that is "concrete and particularized"—meaning it must "actually exist" and "affect the plaintiff in a personal and individual way," rather than being merely "abstract." *Id.* at 338–40.

Rule 12(b)(6). To survive a motion to dismiss under Rule 12(b)(6), a complaint must contain "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). The standard "demands more than an unadorned, the defendant-unlawfully-harmed-me accusation"; mere "labels and conclusions" or a "formulaic recitation of the elements of a cause of action will not do." *Id.* "Dismissal is appropriate under Rule 12(b)(6) where a pleader fails to state a claim upon which relief can be granted." *Underwood v. O'Reilly Auto Parts, Inc.*, 671 F. Supp. 3d 1180, 1187 (D. Nev. 2023) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)).

IV. ARGUMENT

A. Plaintiff Lacks Article III Standing

1. *TransUnion* Precludes Standing Based on a Risk of Future Harm

In *TransUnion*, the Supreme Court unequivocally held that "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm" for purposes of Article III standing. *TransUnion*, 594 U.S. at 436. Rather, plaintiffs may sue only if a "risk of future harm *materializes* and the individual suffers a concrete harm"—in which case "the harm itself, and not the pre-existing risk, will constitute a basis for the person's injury and for damages." *Id.* (emphasis added). *TransUnion's* holding leaves no room for suits predicated on hypothetical future events that may never actually transpire. And here, Plaintiff's primary theory of injury—an alleged "increased risk of additional harm from identity theft and identity fraud," ACAC ¶ 99—is precisely the type of speculative, future-oriented harm that *TransUnion* found insufficient. 594 U.S. at 436.

Plaintiff cannot evade *TransUnion* by labeling the supposed risk of harm as "imminent" or "substantial." ACAC ¶ 67. "Imminency" of a prospective harm is only relevant under *TransUnion* for a claim seeking injunctive relief. *See TransUnion*, 594 U.S. at 435–36 ("a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial") (citations omitted). By contrast, *TransUnion* bars any suit for *damages* premised on the risk of future harm—no matter how substantial that harm may end up being, or how likely it is to occur. Consider the example cited in *TransUnion* itself:

> Suppose that a woman drives home from work a quarter mile ahead of a reckless driver who is dangerously swerving across lanes. The reckless driver has exposed the woman to a risk of future harm, but the risk does not materialize and the woman makes it home safely. As counsel for TransUnion stated, that would ordinarily be cause for celebration, not a lawsuit. But if the reckless driver crashes into the woman's car, the situation would be different, and (assuming a cause of action) the woman could sue the driver for damages.

TransUnion, 594 U.S. at 436–37.

The same principles apply to a data breach lawsuit premised entirely on a claimed risk of future identity theft. Whatever such risk may arise from a data breach, unless and until it actually

materializes—i.e., unless identity theft actually results from the breach—there is no standing to sue for damages. *See I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1051 (N.D. Cal. 2022) ("[I]n light of *TransUnion*, the Court concludes that mere compromise of personal information, without more, fails to satisfy the injury-in-fact element in the absence of an identity theft."); *see also Leonard v. McMenamins, Inc.*, 2022 WL 4017674, at *2 (W.D. Wash. Sept. 2, 2022) ("[T]he theory ... that the threat of identity theft posed by a data breach, without more, can constitute an injury-in-fact – is no longer viable under the Supreme Court's more recent decision in *TransUnion.*"); *see also Dinerstein v. Google, LLC*, 73 F. 4th 502, 515 (7th Cir. 2023) (holding, in case alleging risks from disclosure of plaintiff's data: "*TransUnion* marked a shift in the [Supreme] Court's standing jurisprudence," such that, "[t]o the extent that [the plaintiff] rests his claim for damages on allegations of future risk, the argument is a nonstarter"); *Castro v. Architectural Graphics, Inc.*, 2026 WL 1818974, at *3–4 (E.D. Va. May 21, 2026) (no standing based on a "substantial risk of future identity theft" in breach impacting social security numbers, names, birthdates, and mailing addresses); *Henderson v. Reventics, LLC*, 2024 WL 5241386, at *8 (D. Colo. Sept. 30, 2024) ("a plaintiff does not suffer an injury in fact where the PHI/PII is accessed through a data breach but no direct harm results," notwithstanding theft of social security numbers, sensitive private health information, birthdates, and contact information) (citations omitted); *C.C. v. Med-Data Inc.*, 2022 WL 970862, at *7 (D. Kan. Mar. 31, 2022) (allegations of "imminent, immediate and continuing risk of identity theft" not sufficient for standing in breach involving social security numbers, contact information, and sensitive medical information, where plaintiff did not "allege any misuse of any of the data").

In light of *TransUnion*, Plaintiff is squarely foreclosed from predicating his standing on the supposed risk of identity theft.

2. Any Risk of Future Identity Theft Is Speculative in Any Event

Even if standing could be predicated on a risk of future identity theft—as some courts, applying older Ninth Circuit law, have found despite *TransUnion*—standing on this basis has been found only where the data compromised was of the type that could directly and immediately enable identity theft. *See, e.g., Greenstein v. Noblr Reciprocal Exchange*, 585 F. Supp. 3d 1220, 1227 (N.D.Cal. 2022) (finding that "the injury-in-fact requirement will be satisfied when highly sensitive

personal data, such as social security numbers and credit card numbers, are inappropriately revealed to the public and increase the risk of immediate future harm to the plaintiff") (citing Ninth Circuit decisions pre-dating *TransUnion*, including *Krottner v. Starbucks Corp*., 628 F.3d 1139, 1143 (9th Cir. 2010) and *In re Zappos.com, Inc*., 888 F.3d 1020, 1026 (9th Cir. 2018)). Courts thus routinely deny Article III standing where the impacted data consisted only of less sensitive information—such as names, contact information, and dates of birth. *See, e.g., Kisil v. Illuminate Educ., Inc.*, 2025 WL 2589000 (9th Cir. Sept. 8, 2025) (affirming dismissal on standing grounds where "Plaintiffs [had] not shown that identity theft has occurred" nor was the "kind of information at issue the kind that this court normally considers sufficient to find a credible threat of identity theft," as it did not include "Social Security numbers and financial information") (citations omitted); *Morales v. Conifer Revenue Cycle Sols., LLC*, 2025 WL 1096396, at *4 (C.D. Cal. Mar. 31, 2025) (dismissing claims for lack of standing where data breach only affected "name, date of birth, address" and health insurance-related information, but not "the types of data needed to commit identity theft," like social security numbers and financial account information); *Greenstein*, 585 F. Supp. 3d at 1228 (dismissing claims for lack of standing "because the exposed [personal information] was limited only to Plaintiffs' names, address, and driver's license numbers" that did not pose "an imminent risk of harm"). Standing is lacking in these cases because the supposed risk of harm is speculative, as there is no plausible risk that the data at issue would permit a threat actor to steal someone's identity.

These authorities firmly close the door on Plaintiff establishing standing based on an alleged "increased risk of . . . identity theft and identity fraud." ACAC ¶ 99. No "highly sensitive" information is alleged to have been compromised here that could be used to commit identity theft. Plaintiff alleges that only his "contact information and date[] of birth" were compromised. ACAC ¶ 45. This information is hardly "highly sensitive." People widely disseminate their contact information so that people may contact them. And dates of birth are matters of public record. *See* Restatement (Second) of Torts § 652D cmt. b (Am. L. Inst. 1977) ("There is no liability for giving publicity to facts about the plaintiff's life that are matters of public record, such as the date of his birth."). Moreover, this information is plainly insufficient to enable a bad actor to commit identity theft: one cannot open up a credit line in someone's name or take over their existing financial

accounts merely by knowing their contact information and birthdate. That is why courts have rejected standing in data breach cases in the absence of allegations of more sensitive data being compromised. *See, e.g., Greenstein*, 585 F. Supp. 3d at 1227–29 (no standing because the breached information, which included contact information and dates of birth, was "insufficient to open a new account in Plaintiffs' names or to gain access to personal accounts likely to have more sensitive information"); *Morales* 2025 WL 1096396, at *4 (noting that "less sensitive information … is insufficient [to plead an injury-in-fact] because whether it could be used to commit identity theft is speculative").[1]

Nor can Plaintiff convert these speculative future harms into concrete present harms by alleging he spent time or money to "mitigate" the effects of the Incident. ACAC ¶ 99 (alleging hypothetical "mitigatory actions" that data breach victims may need to take). A plaintiff "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416 (2013). Putting aside that Plaintiff does not even make any specific allegations that he actually spent any time or money trying to "mitigate" the Incident, Plaintiff has not pleaded facts showing an imminent risk of harm that would justify such efforts. Mitigation efforts are only cognizable "when they are based on a risk of harm that is either 'certainly impending' or 'substantial.'" *Zynga,* 600 F. Supp. 3d at 1052 (quoting *Clapper*, 568 U.S. at 422). Where, as here, Plaintiff cannot "show a substantial or imminent risk of identity theft" or other harm, he "cannot rely on the resulting mitigation expenses or emotional distress to secure standing." *Zynga*, 600 F. Supp. 3d 1034 at 1052–54.

Similarly, Plaintiff cannot establish standing based on vague allegations of "anxiety" about the possibility of identity theft. *See, e.g.*, ACAC ¶ 96. "[C]ourts have deemed emotional distress too

---

[1] *See also In re Uber Techs., Inc., Data Sec. Breach Litig.*, 2019 WL 6522843, at *1, 3 (C.D. Cal. Aug. 19, 2019) (no imminent risk of harm when breach involved "names, email addresses, [] mobile phone numbers … [and] driver's license numbers" but "no social security numbers [or] credit card information"); *Antman v. Uber Techs., Inc.,* 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) ("Without a hack of information such as social security numbers, account numbers, or credit card numbers, there is no obvious, credible risk of identity theft that risks real, immediate injury."); *Jackson v. Loews Hotels, Inc.*, 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) (same); *Zynga,* 600 F. Supp. 3d at 1055 (same, even where plaintiffs were minors).

speculative to constitute a measure of damages in data breach cases." *In re Yahoo! Inc. Customer Data Sec. Breach Litig*., 2020 WL 4212811, at *16 (N.D. Cal. July 22, 2020) (citing *Pruchnicki v. Envision Healthcare Corp*, 439 F. Supp. 3d 1226, 1234 (D. Nev. 2020)); *see also Holly v. Alta Newport Hosp., Inc*., 2020 WL 6161457, at *3–4 (C.D. Cal. Oct. 21, 2020) (dismissing negligence claim based on "conclusory and vague" claims of "emotional harm and distress"). This is particularly true here, where Plaintiff has not pleaded facts showing that his private information was actually "exposed" at all, or that the impacted data included any information that could be used to commit any harm in the first place. Under these circumstances, the supposed risk that "caused the asserted . . . stress is too conjectural" to support standing. *Zynga,* 600 F. Supp. 3d at 1052–53.

3. Plaintiff's Remaining Injury Theories Cannot Confer Standing

Aside from theories deriving from the speculative risk of identity theft, the Complaint ticks off a laundry list of additional "injuries," none of which are sufficient to support standing.

"Loss of value" of PII. Plaintiff cannot allege a concrete and particularized injury based on the supposed "diminution of value" of Plaintiff's PII. ACAC ¶ 8. In order to survive a motion to dismiss on this theory of harm, a plaintiff "must establish both the existence of a market for her personal information and an impairment of her ability to participate in that market." *Pruchnicki*, 439 F. Supp. 3d at 1234, *aff'd*, 845 F. App'x 613 (9th Cir. 2021). Plaintiff here alleges neither. First, while the Complaint generically alleges that "[s]tolen PII is often trafficked on the dark web," ACAC ¶ 58, it fails to allege that an economic market exists for the specific information at issue here: basic contact information and dates of birth. Instead, Plaintiff alleges that online marketplaces sell "stolen identity credentials" (*id.* ¶ 61) and PII that can be used to access victims' "bank accounts, social media, credit card, and tax details" and "siphon money from current accounts [or] open new accounts" in victims' names. *Id.* ¶¶ 62, 65. None of this information is alleged to have been affected by the Incident.

Second, nowhere does the Complaint allege that Plaintiff himself participates in any market for selling his contact information or date of birth—which would be patently absurd. People do not "sell" their contact information or birthdates, and Plaintiff makes no specific allegation that he ever did or planned to do so, let alone a plausible one. Accordingly, Plaintiff is in no position to allege

that he "lost" any "value" he otherwise stood to gain from participating in an alleged market for the information taken. One cannot lose market value from something one never planned to sell in the first place. *See Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 46 (D. Ariz. 2021) (applying *Pruchnicki* and finding that "without identifying a market in which they can or could and intend or intended to sell their information, Plaintiffs here fail to demonstrate a loss in value of their PII or PHI"); *Johnson v. Yuma Reg'l Med. Ctr.*, 769 F. Supp. 3d 936, 948 (D. Ariz. 2024) (holding that "Plaintiffs failed to plead a diminution of value" where they did not allege "that they ever have, intend to, or intended to sell" their information on the dark web).

Benefit of the bargain damages. Plaintiff's "benefit of the bargain" theory—that he "overpaid for Caesars' services" based on some (unpled) expectation that Caesars would provide better data security (ACAC ¶ 160)—fails for multiple reasons. For starters, Plaintiff does not even specify what "services" he allegedly "overpaid" for from Caesars. The Complaint merely alleges that Plaintiff was a member of the Caesars Rewards Program and provided his PII in order to "regularly gamble[]" with Caesars. *Id.* ¶ 14. In doing so, Plaintiff received exactly what he bargained for—an opportunity to gamble and to earn rewards (at no cost) based on his participation in the Rewards program. Plaintiff fails to allege facts sufficient to show that he paid for services that "incorporated some particular sum that was understood by both parties to be allocated towards the protection of consumer data," and did not receive what he bargained for. *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 962 n.5 (D. Nev. 2015); *see also Carlsen v. GameStop, Inc.*, 112 F. Supp. 3d 855, 862 (D. Minn. 2015) (no standing for unjust enrichment claim where plaintiff did not show he "bargain[ed] for data privacy/security"); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 30 (D.D.C. 2014) (allegations "that some indeterminate part of [the price] went toward paying for security measures" were "too flimsy to support standing").

Invasion of privacy. Finally, Plaintiff cannot establish standing by alleging that the Incident has subjected him "to embarrassment and depriv[ed] him of any right to privacy." *See* ACAC ¶ 96. These allegations are entirely conclusory and implausible. Plaintiff does not even allege that his information has been posted publicly in any way that could affect his reputation, but in any event it is nonsensical for Plaintiff to claim "embarrassment" from the disclosure merely of his contact

information and birthdate. Likewise, to the extent Plaintiff is attempting to allege that he has suffered a harm closely analogous to a privacy injury cognizable under common law, the alleged facts are wide of the mark. A person's "name, address, [and] date and place of birth" are not "generally considered 'private'" information that could ground a common-law invasion of privacy claim. *Phillips v. U.S. Customs & Border Protection*, 74 F.4th 986, 996 (9th Cir. 2023) (finding that even "names, birthdays, social security numbers, occupations, addresses, social media profiles, and political views and associations" are not "so sensitive that another's access to that information would be highly offensive to a reasonable person, or otherwise give[] rise to reputational harm or injury to privacy interests"); *see also Zynga, Inc.*, 600 F. Supp. 3d at 1049 (finding that "basic contact information" such as email addresses and phone numbers is not private given that it is "designed to be exchanged to facilitate communication,", and that dates of birth are "matters of public record" that cannot support a common-law privacy injury).

Plaintiff cannot claim privacy-based injuries "simply because there was a data breach." *Masterson v. IMA Fin. Grp., Inc*., 2023 WL 8647157, at *7 (D. Kan. Dec. 14, 2023). Yet that is all he ultimately alleges.

B. Plaintiff Lacks Standing for Injunctive Relief

Not only does Plaintiff lack standing to seek damages, he also lacks standing to seek injunctive relief—because he cannot show a "real and immediate threat of repeated injury." *O'Shea v. Littleton*, 414 U.S. 488, 496 (1974). A past data breach, standing alone, does not establish an ongoing or imminent threat of future injury sufficient for prospective relief. *See, e.g., Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *8 (S.D. Cal. Nov. 3, 2016) (finding that Plaintiff lacked standing for injunctive relief on the basis of his "fear of on-going data breaches" and "inten[t] to continue as a customer if his data can be adequately protected"). Likewise, given the nature of the information impacted by the Incident, and the lack of any tangible injury to Plaintiff to date, Plaintiff cannot show an imminent risk of future harm from *this* Incident. *See supra* Section IV.A.2. That failure forecloses any possibility that he could show a "sufficiently imminent and substantial" risk of harm from a future act of identity theft or fraud. *TransUnion*, 594 U.S. at 435.

C. Each of Plaintiff's Claims Should be Dismissed Under Rule 12(b)(6) For Failure to State a Claim

Beyond failing for lack of standing, Plaintiff's claims each fail on the merits.

1. Plaintiff Fails to State a Claim for Negligence or Negligence Per Se

Plaintiff's negligence claim fails because he does not specify any conduct that could constitute a breach of a duty of care owed by Caesars or plead any cognizable damages.[2]

a. Plaintiff Does Not Allege a Breach of Duty

To plausibly allege a breach of a negligence duty, Plaintiff cannot simply assert that unauthorized access to his PII occurred: he must allege facts sufficient to show how Caesars' data security measures were inadequate. Plaintiff's claim rests on the notion that Caesars "fail[ed] to implement reasonable measures to safeguard" the stolen information and "prevent unauthorized disclosure of that information." ACAC ¶ 6. Yet Plaintiff fails to plead a single fact indicating that Caesars actually had the "woefully inadequate security measures" he claims. *Id.* In paragraphs 68 through 82 of the Complaint, for example, Plaintiff cites a series of regulatory guidelines, standards, and "best practices"—and then conclusorily alleges that Caesars "failed to follow these and other industry standards to adequately protect" Plaintiff's information. But Plaintiff never identifies the security practices he believes were inadequate or explain "[w]hat facts lead [him] to believe [Caesars] didn't comply with industry standards." *Razuki v. Caliber Home Loans, Inc.*, 2018 WL 6018361, at *2 (S.D. Cal. Nov. 15, 2018).

In essence, Plaintiff's theory is simply "that because data was hacked," Caesars' "protections *must* have been inadequate." *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 717 (8th Cir. 2017) (emphasis added) (citation omitted); *see also Johnson*, 769 F. Supp. 3d at 954 (finding no breach of duty where "Plaintiffs' allegations rely on speculation that, had [Defendant] used the industry standards, the breach would not have occurred."). That kind of "naked assertion" in a data-breach case "cannot survive a motion to dismiss." *Kuhns*, 868 F.3d at 717; *accord In re MCG Health Data Sec. Issue*

[2] Under Nevada law, a negligence claim requires "four elements: (1) the existence of a duty of care, (2) breach of that duty, (3) legal causation, and (4) damages." *Sanchez ex rel. Sanchez v. Wal-Mart Stores, Inc.*, 125 Nev. 818, 824 (2009) (citation omitted).

Litig., 2023 WL 3057428, at *3 (W.D. Wash. Mar. 27, 2023); *Griffey*, 562 F. Supp. 3d at 50 ("[T]he existence of an adequate data security infrastructure and two data breaches in a year are not mutually exclusive."); *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1226 (N.D. Ga. 2019) ("[T]he occurrence of a data breach does not necessarily imply that a company's data security is inadequate."). A cyberattack is "merely consistent with" negligence; it does not present "enough pleaded facts to plausibly suggest" wrongdoing. *Bates v. Green Farms Condo. Ass'n*, 958 F.3d 470, 480 (6th Cir. 2020). Data-breach plaintiffs must allege more—and there is nothing more here. *See, e.g.*, *In re Equifax, Inc., Consumer Data Security Breach Litig.*, 362 F. Supp. 3d at 1309–10 (N.D. Ga. 2019) (detailed allegations of "a serious vulnerability" and numerous "warnings" about it); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 388–89 (E.D. Va. 2020).

b. Negligence *Per Se* Fails

To the extent Plaintiff attempts to plead a breach of duty under the doctrine of negligence *per se* based on alleged violations of the FTC Act or Nevada's data privacy law, Nev. Rev. Stat. § 603A.210(1), those efforts fail as a matter of law. "Under a theory of negligence per se, a plaintiff must allege that . . . he or she belongs to a class of persons that a statute is intended to protect." *InjuryLoans.com, LLC v. Buenrostro*, 529 F. Supp. 3d 1178, 1185–86 (D. Nev. 2021). Plaintiff's reliance on Section 603A.210(1) collapses on this basis: the statute "is intended to protect" only *Nevada residents*, and Plaintiff is a *Texas* citizen. ACAC ¶ 14; *see* Nev. Rev. Stat. § 603A.210(1) ("A data collector that maintains records which contain personal information *of a resident of this State* shall implement and maintain reasonable security measures to protect those records").

Similarly, the FTC Act "does not recognize a private right of action" and therefore cannot serve as a negligence per se predicate. *Baton v. Ledger SAS*, 740 F.Supp.3d 847, 912 (N.D. Cal. 2024) (citation omitted); *see also InjuryLoans.com, LLC v. Buenrostro*, 529 F. Supp. 3d 1178, 1185–86 (D. Nev. 2021) (dismissing negligence per se claims based on federal statutes because plaintiffs could not maintain a private right of action under the Bank Secrecy Act, Patriot Act, and the associated regulations either independently or under a theory of negligence per se); *Shah v. Cap. One Fin. Corp.*, 768 F.Supp.3d 1033, 1045 (N.D. Cal. 2025) (noting that "district courts do not permit negligence per se claims to hinge on the FTC Act.").

c. Plaintiff Fails to Allege Cognizable Damages

Independent of standing, Plaintiff fails to allege any type of damages cognizable under state negligence law. To sustain a claim for negligence, Plaintiff must allege "cognizable damages" as a result of Caesars' conduct. *Pruchnicki*, 439 F. Supp. 3d at 1231. Alleged injuries that "stem from the danger of future harm" are insufficient to support a negligence claim. *Krottner*, 406 F. App'x at 131 (9th Cir. 2010) (dismissing negligence claim under Washington law); *see also Pruchnicki*, 845 F. App'x. at 614 ("Although [plaintiff] alleged sufficient injury-in fact to support standing, whether the allegations adequately alleged compensable damages is a different question."); *Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686, 695–96 (N.D. Cal. 2019) (while standing was present, allegations claiming an increased risk of future identity theft did "not rise to the level of appreciable harm to assert a negligence claim" under California law) (citation omitted). Plaintiff must instead plead "nonspeculative," "appreciable and actual damage." *Ruiz v. Gap, Inc.*, 380 F. App'x 689, 691–92 (9th Cir. 2010).

As discussed *supra*, Section IV.A.1, Plaintiff does not allege that he personally incurred any actual damage at all. For example, he does not allege to have experienced any actual fraud or identity theft, or to have incurred any out-of-pocket losses or mitigation expenses. That is dispositive. Where "personal information is compromised due to a security breach, there is no cognizable harm absent actual fraud or identity theft." *Grigsby v. Valve Corp.*, 2012 WL 5993755, at *2 (W.D. Wash. Nov. 14, 2012) (dismissing negligence claim); *see also Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 917–18 (N.D. Cal. 2009) (no actionable contract or negligence injury when plaintiff "has no actual damages to mitigate since he has never been a victim of identity theft"); *Pruchnicki*, 845 F. App'x. at 615 (dismissing claims for negligence, implied contract, and deceptive practices where the plaintiff had not alleged that she suffered identity theft or fraud or any out-of-pocket losses supported by non-conclusory allegations). Nor can Plaintiff rely on an increased risk of future harm as the basis for his negligence claim, as that risk is "too tenuous to constitute 'damages' as an element of plaintiff's claims" given the nature of the information involved in the Incident. *Pruchnicki*, 439 F. Supp. 3d at 1231.

/ / /

Plaintiff's remaining damages theories are not cognizable in tort. The Complaint purports to seek recovery of "time, resources, and money spent on mitigation efforts," ACAC ¶ 133, but Plaintiff does not allege facts sufficient to show that he incurred any mitigation costs or that it was necessary to devote any of his time to activities like "monitor[ing his] financial and other accounts" when the breach was limited to contact information and Plaintiff's date of birth. *See Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273, 284 (S.D.N.Y. 2008) (courts "have uniformly ruled" that time and expense combatting increased risks of future identity theft is not "an injury that the law is prepared to remedy"); *Pruchnicki*, 439 F. Supp. 3d at 1233 (plaintiffs "who claim only that they may incur expenses in the future have not" pled cognizable injuries). Plaintiff's alleged "anxiety, annoyance, and nuisance", ACAC ¶¶ 8, 100, likewise cannot constitute cognizable injury under Nevada law, because "in the absence of physical impact, proof of serious emotional distress causing physical injury or illness must be presented." *Pruchnicki*, 845 F. App'x at 614; *see also In re Eureka Casino Breach Litig.*, 2024 WL 4253198, at *3 (D. Nev. Sept. 19, 2024) ("anxiety about unauthorized parties viewing, selling, and/or using … Private Information for purposes of identity theft and fraud" does not constitute "physical injury or even serious emotional distress"). Finally, Plaintiff's claim that his information "lost value" is just as deficient as a measure of tort damages. *See, e.g., Pruchnicki*, 439 F. Supp. 3d at 1235–1236 (rejecting diminution of value as a viable tort damages theory where plaintiff did not allege that the information at issue had been disclosed or the breach "otherwise impeded her ability to participate in the market").

d. Plaintiff's Purported Damages Are Barred by the Economic Loss Doctrine

The economic loss doctrine independently bars Plaintiff's negligence claim for purely economic damages. Nevada law provides "that unless there is personal injury or property damage, a plaintiff may not recover in negligence for economic losses." *Terracon Consultants W., Inc. v. Mandalay Resort Grp.*, 125 Nev. 66, 87 (2009) (citation omitted). This rule is based on Nevada's policy recognizing "the need for useful commercial economic activity," *id.*, and "protects parties from unlimited economic liability" that could otherwise arise from unintentional torts in commercial settings. *Halcrow, Inc. v. Eighth Jud. Dist. Ct.*, 129 Nev. 394, 399 (2013). The harms Plaintiff alleges

in support of his negligence claim are insufficient, but even if the alleged harms are considered, they nearly all constitute paradigmatic economic losses. *See* ACAC ¶¶ 8, 133-134 (seeking damages based on diminution of the value of private information, credit monitoring costs, and unspecified out-of-pocket expenses). Plaintiff also vaguely refers to "time spent" dealing with the Incident; setting aside the conclusory nature of that allegation, it is likewise considered an economic harm because it "implicitly refer[s] to the [] time's financial value." *Moore v. Centrelake Med. Grp., Inc.*, 299 Cal. App. 5th 515, 536 (2022). And to the extent that Plaintiff does attempt to allege noneconomic injuries—such as conclusory allegations concerning "anxiety, annoyance, and nuisance", ACAC ¶ 8—such injuries are nothing more than "'naked assertions' devoid of 'further factual enhancement'" that cannot survive Rule 8's pleading standard. *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 557).

2. Plaintiff Fails to State a Claim for Breach of Implied Contract

"Nevada law requires the plaintiff in a breach of contract action to show: (1) the existence of a valid contract; (2) a breach by the defendant; and (3) damage as a result of the breach." *Smallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1195 (D. Nev. 2022). Plaintiff does not plausibly plead any of these elements.

a. No Breach of an Identified Contractual Term

Plaintiff's breach of implied contract claim fails at the threshold because Plaintiff does not adequately allege the existence of an implied contract or any of its terms. Regarding formation, Plaintiff vaguely alleges that he was "required to provide [his] PII" to purchase "services" from Caesars (ACAC ¶ 138), but the Complaint never explains what "services" Plaintiff bargained for in exchange. Elsewhere, Plaintiff alleges that Caesars required customers to "provide their PII during the reservation and/or check-in process" (*id.* ¶ 140), but Plaintiff does not allege he was ever a hotel guest or provided his PII as part of that process. To the extent Plaintiff simply provided his PII in the course of gambling with Caesars, that is insufficient to create an implied contract with respect to that data. *See, e.g., In re Mednax Servs., Inc. Customer Data Sec. Breach Litig.*, 603 F. Supp. 3d 1183, 1221 (S.D. Fla. 2022) (noting that, while some courts have found an implied contract to exist where "consumers are solicited or invited to provide personal information in exchange for a good or

service," no contract existed where plaintiffs only "provided their personal information as required to receive healthcare services" from the defendants—"not data security services"); *Shah* 768 F. Supp. 3d at 1050 (dismissing breach of implied contract to provide adequate data security services where plaintiffs "fail to expand on the nature of the implied contact" or how it was formed).

Plaintiff also fails to identify a specific contractual term that Caesars allegedly breached. Plaintiff vaguely alleges that "Caesars impliedly promised to adopt reasonable data security measures" and that "Caesars made implied or implicit promises that its data security practices were reasonably sufficient to protect consumers' PII." ACAC ¶ 140. But the Complaint does not explain the origin of these purported promises and does not identify any other "specific term[] of the implied contracts" that Caesars allegedly breached. *Griffey,* 562 F. Supp. 3d at 51. To the extent Plaintiff's claim is based on statements made in Caesars' Privacy Policy—which is not specifically alleged—the claim necessarily fails because Plaintiff does not (and cannot) identify any promise that Caesars would maintain perfect data security or that no breach could ever occur. *See Kuhns*, 868 F.3d at 717 ("[Plaintiff] does not allege that Scottrade affirmatively promised that its customer data would not be hacked, and such a promise may not be plausibly implied."); *Flores v. United Parcel Serv., Inc*., 768 F. App'x 677, 679 (9th Cir. 2019) (affirming dismissal of contract claim where "documents 'contain[] no promissory language' that would oblige UPS to use a particular mode of transportation").

Nor are Plaintiff's conclusory allegations that "Caesars breached its implied contracts . . . by failing to implement reasonable data security measures" sufficient. ACAC ¶ 144. Plaintiff does not allege how Caesars violated this alleged promise other than the fact that the data breach occurred. As detailed above, the claim that a company "fail[ed] to implement reasonable data security measures" "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 [Caesars'] protections must have been inadequate is a naked assertion[] devoid of further factual enhancement that cannot survive a motion to dismiss." *Id*. (citations omitted). Beyond that "naked assertion," Plaintiff's "vague allegations do not establish how [Caesars] failed to take reasonable measures to protect customer's data." *Gardiner*

v. Walmart Inc., 2021 WL 2520103, at *6 (N.D. Cal. Mar. 5, 2021); *see also Razuki v. Caliber Home Loans, Inc*, 2018 WL 2761818, at *3 (S.D. Cal. June 8, 2018).

Finally, Plaintiff also does not allege that he read, reviewed, or relied upon any specific term of the Privacy Policy or any other Caesars communication in deciding to provide his personal information. Nor does Plaintiff allege that he would have ceased using Caesars services had he known of any purported security deficiency. These deficiencies likewise provide reason to dismiss Plaintiff's claim. *See Krottner*, 406 F. App'x at 131 (where plaintiffs claimed that the terms of a contract were defined by three documents, there was no contract formed where plaintiffs failed to "allege that they read or even saw the documents").

b. No Cognizable Damages

As stated above, Plaintiff fails to show cognizable damages, which he must demonstrate to support a contract claim. *Pruchnicki*, 439 F. Supp. 3d at 1236. (dismissing implied contract claim in data breach context for lack of damages). Where (as here) Plaintiff "does not allege any out-of-pocket expenses related to the underlying data breach" that were necessarily incurred, he cannot support the damages element of his contract claim. *Id*. at 1234; *see supra* at Section IV.C.1.c. Plaintiff's breach of implied contract claim fails for this independent reason.

3. Plaintiff Does Not Plead a Viable Unjust Enrichment Claim

To state an unjust enrichment claim, Plaintiff 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. Apr. 1, 2019) (citation omitted). Plaintiff cannot make out an unjust enrichment claim here.

First, unjust enrichment is a form of equitable relief, which Plaintiff cannot seek because he does not plead a lack of legal remedies. As the Ninth Circuit has held in *Sonner v. Premier Nutrition Corporation*, under federal law, plaintiffs cannot pursue equitable remedies unless they can show they lack an adequate remedy at law. 971 F.3d 834, 845 (9th Cir. 2020) ("[W]hen a plain, adequate, and complete remedy exists at law, we hold that federal courts rely on federal equitable principles before allowing equitable restitution in such circumstances."). Unjust enrichment is equitable in

nature. *H&H Pharm. Co. v. Chattem Chems., Inc.*, 2020 WL 376648, at *15 (D. Nev. Jan. 23, 2020). So, too, is the remedy of disgorgement, which Plaintiff expressly seeks. ACAC ¶ 160; *see also JL Beverage Co., LLC v. Beam Inc*., 2017 WL 5158661, at *2 (D. Nev. Nov. 7, 2017) ("disgorgement is an equitable remedy"). Plaintiff makes no allegation sufficient to show that he lacks an adequate remedy at law in order to pursue these remedies. To the contrary, Plaintiff seeks "all forms of monetary compensation" for each of his three remaining claims, which are based on the *same conduct* underlying his putative unjust enrichment claim. *See* ACAC ¶¶ 135, 146, 170–171. Plaintiff makes a passing allegation that he has "no adequate remedy at law" because Caesars "continues to retain [his] PII while exposing the PII to a risk of future data breaches." ACAC ¶ 158. But even here, the "remedy [] sought by Plaintiff[] ultimately is money damages." *Smallman*, 638 F. Supp. 3d at 1198.[3] Because Plaintiff has not shown he lacks legal remedies, his unjust enrichment claims are barred by *Sonner*. *See, e.g., Sharma v. Volkswagen AG*, 524 F. Supp.3d 891, 909 (N.D. Cal. 2021) ("Because they have not shown that legal remedies are unavailable or inadequate as to either past or future injury, Plaintiffs' CLRA UCL, and unjust enrichment claims must be dismissed.").

Second, Plaintiff fails to plead that he conferred any "benefit" on Caesars that was "unjustly" retained. Plaintiff's bare allegation that he "conferred monetary benefits on Caesars" cannot suffice. ACAC ¶ 149. The only interaction with Caesars that Plaintiff alleges is that he "regularly gambled" online and at Caesars properties. *Id.* ¶ 14. But Plaintiff does not claim that Caesars failed to provide a benefit in return—i.e., the gambling services that Plaintiff sought. Nor does Plaintiff suggest that he was somehow charged a premium for those services in exchange for data security services. *See, e.g., Crowe v. Managed Care of N. Am., Inc.*, 2024 WL 6863341, at *9 (S.D. Fla. Aug. 16, 2024) ("In pleading an unjust enrichment claim in the data breach context, Courts have required plaintiffs to allege that defendants charged plaintiffs a premium for data security"). Plaintiff alternatively suggests that Caesars profited in unspecified ways simply by receiving PII. ACAC ¶ 151. But this

[3] As in *Smallman*, Plaintiff here seeks "prospective damages for the continued profit Defendant [Caesars allegedly] derives from the use of Plaintiffs' PII"—i.e., monetary damages tied to Caesars' continued "retention" of Plaintiff's information. *Id.* at 1198 (dismissing unjust enrichment claim); ACAC ¶ 151 (alleging that Caesars uses PII for "a variety of profit-generating purposes" including "to generate future stays" and "derive further revenues and profits").

theory requires that the information itself had "independent monetary value" that Caesars actually retained the benefits from. *In re Arthur J. Gallagher Data Breach Litig*., 631 F. Supp. 3d 573, 592 (N.D. Ill. 2022); *see also In re Zappos.com*, 2013 WL 4830497, at *5 (D. Nev. Sept. 9, 2013) (dismissing unjust enrichment claim in data breach case because customers did not "bestow[] any gratuitous benefit upon Defendant" by simply providing their PII). Plaintiff fails to allege that Caesars somehow sold or otherwise profited from the use of Plaintiff's PII. And in any event, Plaintiff has failed to allege facts showing that any purported enrichment based on the provision of his PII was at *Plaintiff's expense*. *See, e.g., Karupaiyan v. Expertis IT*, 2022 WL 4280529, at *5 (S.D.N.Y. Sept. 15, 2022) (dismissing unjust enrichment claim where plaintiff failed to show defendants retained a benefit at his expense). Even assuming *arguendo* that Caesars derived some unspecified "value" of Plaintiff's information, Plaintiff fails to allege that after providing this information, he could no longer use or monetize that information. *See, e.g., Mount v. PulsePoint, Inc.*, 2016 WL 5080131, at *6 (S.D.N.Y. Aug. 17, 2016) (rejecting unjust enrichment claim based on alleged misappropriation of the value of plaintiffs' information where there was no alleged loss or deprivation of opportunity); *aff'd*, 684 F. App'x 32 (2d Cir. 2017). The unjust enrichment claim should be dismissed.

4. Plaintiff Fails to State a Nevada Consumer Fraud Act Claim

Plaintiff's Nevada Consumer Fraud Act claim should be dismissed because Plaintiff attempts to recast a criminal data security incident as consumer fraud, but cannot plead a *knowing*, actionable omission or predicate statutory violation. To state a claim under the Nevada Consumer Fraud Act, Plaintiff must "prove that (1) an act of consumer fraud by the defendant (2) caused (3) damage to the plaintiff." *Whittum v. Acceptance Now*, 2019 WL 4781846, at *3 (D. Nev. Sept. 30, 2019). Because this claim sounds in fraud, Plaintiff must plead the facts to support it with particularity under Rule 9(b). *See Allstate Ins. Co. v. Belsky*, 2017 WL 7199651, at *7 (D. Nev. Mar. 31, 2017) ("Consumer fraud claims brought under this [NCFA] statute are subject to Rule 9(b)'s heightened pleading requirements"); *Davenport v. Homecomings Fin., LLC*, 2014 WL 1318964, slip op. at *3 (D. Nev. Mar. 31, 2014) (similar).

/ / /

Plaintiff predicates his consumer fraud claim on two statutory prongs: that Caesars (i) "knowingly . . . [f]ail[ed] to disclose a material fact in connection with the sale or lease of goods or services" (Nev. Rev. Stat. § 598.0923(1)(b)); and (ii) "knowingly . . . [v]iolate[d] a state or federal statute or regulation relating to the sale or lease of . . . services." Nev. Rev. Stat. § 598.0923(1)(c). Neither theory is viably pled.

No material omission. Plaintiff's fraud allegations are premised entirely on an omission theory. *See* ACAC ¶ 163 (alleging that Caesars "failed to disclose the material fact that its data security procedures were deficient"). To succeed on that theory, Plaintiff must show Caesars had an affirmative duty to disclose the allegedly omitted information. *Taddeo v. Taddeo*, 2011 WL 4074433, at *6 n.3 (D. Nev. Sept. 13, 2011); *see also Soffer v. Five Mile Cap. Partners, LLC*, 2013 WL 638832, at *10 (D. Nev. Feb. 19, 2013) ("For a mere omission to constitute actionable fraud" in Nevada, Plaintiff "must first demonstrate that [Caesars] had a duty to disclose the fact at issue."). Plaintiff, however, pleads no facts establishing any duty to disclose on the part of Caesars, such as a "fiduciary relationship." *Soffer*, 2013 WL 638832, at *10. Rather, Plaintiff's relationship with Caesars was strictly a commercial one—he "regularly gambled" as a customer of Caesars. ACAC ¶ 14; *see also In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d at 1337 (dismissing Nevada Consumer Fraud Act claim predicated on omissions theory: "In the absence of a confidential relationship, no duty to disclose exists when parties are engaged in arm's-length business negotiations; in fact, an arm's length relationship by its nature excludes a confidential relationship.").

Even if a duty to disclose were to exist, Plaintiff fails to allege any *specific facts* about data security deficiencies that Caesars allegedly failed to disclose. The Complaint merely states in conclusory fashion that Caesars' failed to disclose that its "data security practices" were "deficient" and its "cloud security settings" were "not adequate." ACAC ¶ 163. Mere allegations that a defendant failed to disclose that its security systems were not 100% secure or that it could not guarantee protection against a data breach are insufficient as a matter of law. And any such claim would contradict the Privacy Policy in any event, which disclosed only that Caesars employed "reasonabl[e] and "appropriat[e]" security measures and—in the very next sentence—warned that

"Caesars cannot guarantee or warrant the security of any [consumer] information" transmitted to Caesars. ACAC ¶ 32; *see, e.g., Yuille v. Uphold HQ Inc*., 686 F. Supp. 3d 323, 347–48 (S.D.N.Y. 2023) (dismissing claim where reframing statements as omissions "could not have communicated the impression that [the] platform was so secure that no hackers, no matter how talented, could penetrate [the] platform"); *In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 542 (M.D. Pa. 2021) (determining that the omission-based claims could not be squared away with allegations in the complaint about similar misrepresentations).

Plaintiff's omission-based theory also fails because Plaintiff does not plausibly allege that Caesars had knowledge of any undisclosed security deficiencies. The Complaint alleges in conclusory fashion that Caesars "was aware that the hotel industry was a frequent target of sophisticated cyberattacks" and "should have known that its cloud server data services practices" were "insufficient." ACAC ¶ 163. But Plaintiff fails to allege any facts that Caesars somehow knew of any specific security deficiencies—rather than generic threats to the industry at large—much less deficiencies that enabled the Incident and that Caesars deliberately withheld from Plaintiff. The Complaint's allegations do not even approach what is required to meet Rule 9(b).

No violations of other statutes. Plaintiff's secondary theory is that Caesars' alleged violations of other state and federal statutes also establish a claim under the Nevada CFA. Not so. To base a Nevada CFA claim on the violation of another statute, Plaintiff must "plead with particularity how the facts of this case pertain to that specific statute." *See Baba v. Hewlett-Packard Co*., 2010 WL2486353, at *6 (N.D. Cal. June 16, 2010) (citation omitted). Plaintiff first claims that Caesars violated Nev. Rev. Stat. § 603A.210(1), which requires businesses to "implement and maintain reasonable security measures" to protect the PII of Nevada residents in their possession. ACAC ¶ 165. But again, that statute applies only to Nevada residents, and Plaintiff resides in Texas. Nev. Rev. Stat. § 603A.210(1) (coverage limited to "personal information of a *resident of this State*") (emphasis added). Plaintiff falls back on allegations that Caesars violated the FTC Act, but his vague and conclusory references to that statute miss the mark. ACAC ¶ 167. Plaintiff fails to plead specific facts concerning how Caesars "knew or should have known that its data security practices were deficient," how it "violated the FTC Act," or how it "failed to adhere to the FTC's data security

guidance." *Id*. For example, Plaintiff does not say what guidance Caesars failed to adhere to, how Caesars failed to adhere to it, how the alleged failure resulted in the Incident occurring, and how the alleged failures harmed Plaintiff. This is the type of conclusory allegation prohibited by *Twombly* and *Iqbal*. Indeed, allowing Plaintiff's deficient pleading to go forward here would mean every business victimized by a data breach would be deemed to have violated the FTC Act, as virtually every industry has been the "target of sophisticated cyberattacks." ACAC ¶ 165. That is not the law.

V. CONCLUSION

For the foregoing reasons, Caesars requests that this Court dismiss the Amended Class Action Complaint with prejudice.

DATED: July 22, 2026.

McDONALD CARANO LLP

/s/ Adam Hosmer-Henner
Adam Hosmer-Henner (NSBN 12779)
Chelsea Latino (NSBN 14227)
Jane Susskind (NSBN 15099)
100 West Liberty Street, Tenth Floor
Reno, Nevada 89501
ahosmerhenner@mcdonaldcarano.com
clatino@mcdonaldcarano.com
jsusskind@mcdonaldcarano.com

LATHAM & WATKINS LLP
Serrin Turner (*Pro Hac Vice*)
1271 Avenue of the Americas
New York, New York 10022
serrin.turner@lw.com

Attorneys for Defendant Caesars Entertainment, Inc.