UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

In re: DATA BREACH SECURITY LITIGATION AGAINST CAESARS ENTERTAINMENT, INC.

Case No. 2:23-cv-01447-ART-BNW

ORDER DENYING DEFENDANT'S MOTION TO DISMISS
(ECF No. 91)

This is a consolidated class action against Defendant Caesars Entertainment, Inc. ("Caesars") relating to a data breach. In August 2023, Caesars' Rewards member database was hacked, and Plaintiffs' personal identifying information ("PII") was accessed by hackers. Plaintiffs were members of Caesars' rewards program and/or customers of Caesars' gaming and entertainment services at the time. Plaintiffs bring a putative class action seeking redress for the harms they allegedly suffered from the data breach. (*See* ECF No. 81 ("Consolidated Class Action Complaint").)

Before the Court is Defendant's motion to dismiss for lack of standing and failure to state a claim. (ECF No. 91.) For the following reasons, the Court finds that Plaintiffs have standing, and that Plaintiffs have plausibly pled each of their claims. Accordingly, Defendant's motion to dismiss is denied.

I. BACKGROUND

A. Summary of Allegations

On or around August 18, 2023, members of the cybercriminal group Scattered Spider gained access to Caesars' loyalty program database through a social engineering attack on Caesars' IT support company.[1] (ECF No. 81 at ¶¶ 2,

[1] Plaintiffs' lawsuit against that company, Coforge, Ltd. ("Coforge"), has since

224, 225.) The database contained sensitive PII, including names, drivers' license numbers, and social security numbers of a "significant number" of Caesars' loyalty program's 65 million members. (ECF No. 81 at ¶ 1.) Caesars identified the suspicious activity on that day, yet Scattered Spider downloaded the PII five days later. (*Id.* at ¶ 225.)

On September 7, 2023, Caesars' interval investigation confirmed that Scattered Spider had acquired, among other data, a copy of its loyalty program database including names, driver's license numbers, and social security numbers for "a significant number of Caesars Rewards' tens of millions of members." (*Id.* at ¶ 227.) On or around September 14, 2023, Caesars filed a Form 8-K with the SEC to alert investors and shareholders that the data breach had occurred. (*Id.* at ¶ 228.) Caesars also put up a website about the breach, which acknowledged that at a minimum the driver's license numbers and social security numbers of Caesars Rewards members had been accessed and copied. (*Id.* at ¶ 228.)

B. Caesars' Rewards Program

Caesars is one of the world's largest lodging and gaming companies and considers itself a global leader in gaming and hospitality. (*Id.* at ¶ 3.) Its loyalty program, Caesars Rewards, allows members to earn credits by gambling or staying at Caesars' properties. (*Id.* at ¶¶ 3–4, 210.) Caesars requires that its members provide highly sensitive PII such as their full legal name, full address, date of birth, drivers' license number, and social security number. (*Id.* at ¶ 212.) Caesars' 2023 Privacy Policy promises to "maintain physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse, and alteration of the information under [their] control." (*Id.* at ¶¶ 215, 239.)

---

been consolidated with this case, but the present motion concerns only Caesars. (ECF No. 130.)

Caesars was aware that it faced a significant risk of cyberattacks well before the August 2023 attack. (*Id.* at ¶¶ 250, 251.) Caesars told investors in 2022 that: "Compromises of our information systems or unauthorized access to confidential information or our customers' personal information could materially harm our reputation and business." (*Id.* at ¶ 250.) Plaintiffs allege that despite knowing those risks, Caesars failed to adopt reasonable safeguards to protect their PII. (*Id.* at ¶ 251.)

C. Plaintiffs' Harm

Plaintiffs allege that as a result of the data breach, they have experienced "actual and attempted fraud and/or have been exposed to an increased risk of fraud, identity theft, and other misuse of their PII." (*Id.* at ¶ 10.) They now closely monitor their financial and other accounts to guard against fraud, which is burdensome and time-consuming. (*Id.*) Plaintiffs also have already or will purchase credit monitoring and other identity protection services, purchase credit reports, place credit freezes and fraud alerts on their credit reports and spend time investigating and disputing fraudulent or suspicious activity on their accounts. (*Id.*) One Plaintiff has already spent $400 for a one-year subscription for identity protection services. (*Id.* at 16.) Although Caesars offered to provide credit monitoring to its loyalty program members, it has only agreed to provide that service for 24 months. (*Id.* at ¶ 294.)

Several Plaintiffs have discovered that their PII was for sale on the dark web following the data breach. (*Id.* at ¶¶ 6, 20, 41, 51, 61, 82, 92, 118, 140, 170, 191, 273.) Plaintiffs allege that this stolen PII can be used on its own or in combination with personal information from other sources to create a package of information capable of being used to commit further identity theft. (*Id.* at ¶ 11.) Plaintiffs also allege that, had they known that the purchases at Caesars did not include adequate data security, they would have paid less or not stayed at

Caesars hotels. (*Id.* at ¶ 290.) Plaintiffs also allege that the value of their PII has diminished as a result of the data breach. (*Id.* at ¶¶ 276–85.)

D. Class Plaintiffs

There are nine proposed classes in this case: Nationwide Class; California Subclass; Illinois Subclass; Indiana Subclass; Minnesota Subclass; New York Subclass; Pennsylvania Subclass; Texas Subclass; and Virginia Subclass. (*Id.* at ¶¶ 308, 312.) The Nationwide Class asserts claims against Caesars for negligence (Count I), breach of implied contract (Count II), unjust enrichment (Count III), and violation of the Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600 (Count IV). (*Id.* at ¶ 309.) The statewide subclasses assert statutory claims for violations of various state data breach notification and consumer protection statutes. (Counts V–XVIII).

E. Procedural History

Plaintiffs filed the initial class action complaint in this case in September 2023. (ECF No. 1.) Other lawsuits relating to the same data breach were subsequently consolidated into this case. (ECF Nos. 21, 46, 55.) In July 2024, Plaintiffs filed the Consolidated Class Action Complaint. (ECF No. 81.) Caesars moves to dismiss all claims in that complaint. (ECF No. 91.) Also before the Court is Plaintiffs' motion for leave to file supplemental authorities in support of its opposition to the motion to dismiss (ECF No. 114), which the Court grants and considers in this order.

II. LEGAL STANDARD

A. Article III Standing

Under Rule 12(b)(1), a party may move to dismiss for lack of subject matter jurisdiction. "[L]ack of Article III standing requires dismissal for lack of subject matter jurisdiction under [Rule] 12(b)(1)." *Maya v. Centex Corp.*, 658 F.3d 1060, 1067 (9th Cir. 2011). The "irreducible constitutional minimum" of standing

requires that a "plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330 (2016). Injury in fact requires "an invasion of a legally protected interest which is (a) concrete and particularized," and "(b) 'actual or imminent, not conjectural or hypothetical.'" *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992) (citations omitted). "The party invoking federal jurisdiction bears the burden of establishing these elements . . . with the manner and degree of evidence required at the successive stages of litigation." *Id.* at 561. At the pleading stage, "[g]eneral allegations" of injury may suffice. *Id.*

B. 12(b)(6)

An initial pleading must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a). The court may dismiss a complaint for "failure to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). In ruling on a motion to dismiss, "[a]ll well-pleaded allegations of material fact in the complaint are accepted as true and are construed in the light most favorable to the non-moving party." *Faulkner v. ADT Sec. Servs., Inc.*, 706 F.3d 1017, 1019 (9th Cir. 2013) (citations omitted).

To survive a motion to dismiss, a complaint need not contain "detailed factual allegations," but it must do more than assert "labels and conclusions" or "a formulaic recitation of the elements of a cause of action . . . ." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)). In other words, a claim will not be dismissed if it contains "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face," meaning that the court can reasonably infer "that the defendant is liable for the misconduct alleged." *Id.* (internal quotation and citation omitted). The Ninth Circuit, in elaborating on the pleading standard described in *Twombly* and

Iqbal, has held that for a complaint to survive dismissal, the plaintiff must allege non-conclusory facts that, together with reasonable inferences from those facts, are "plausibly suggestive of a claim entitling the plaintiff to relief." *Moss v. U.S. Secret Serv.*, 572 F.3d 962, 969 (9th Cir. 2009).

III. DISCUSSION

A. Article III Standing

Caesars contends that Plaintiffs lack Article III standing because Plaintiffs cannot establish "injury in fact" and because Plaintiffs cannot establish that their injury is "fairly traceable" to Caesars' actions. (ECF No. 91 at 19–26.) The Court addresses each argument in turn.

1. Injury In Fact

Plaintiffs allege that they have suffered several types of injuries, including imminent risk of identity theft, actual or attempted fraud, loss of value of PII, benefit of the bargain damages, and mitigation efforts. Caesars primarily challenges Plaintiffs' first theory of injury: risk of identity theft. Caesars argues that this does not confer Article III standing because Plaintiffs allege only risk of future harm, pointing to *TransUnion LLC v. Ramirez*, 594 U.S. 413, 436 (2021). (ECF No. 91 at 19.) Plaintiffs argue that allegations of a credible threat of real and immediate harm stemming from the theft of their personal information are sufficient to establish injury in fact under *In re Zappos.com, Inc.*, 888 F.3d 1020, 1027 (9th Cir. 2018) and *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010). (ECF No. 96 at 15–19.) Caesars contends that those cases "are no longer good law" after *TransUnion*. (ECF No. 102 at 8–9.)

In *TransUnion*, the Court addressed whether a group of consumers who had misleading alerts in their credit reports had standing to sue. 594 U.S. at 417. The Court distinguished between plaintiffs whose credit reports were disseminated to third parties and plaintiffs whose credit reports were maintained

internally. *Id.* The Court held that the plaintiffs whose credit reports were disseminated to third parties suffered a concrete injury in fact under Article III. *Id.* at 433. The plaintiffs whose credit reports were not disseminated lacked standing because "[t]he mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm." *Id.*

i. Imminent Risk of Identity Theft

Following *TransUnion*, "courts across the country have recognized that harms that result as a consequence of a plaintiff's knowledge of a substantial risk of identity theft, including time and money spent responding to a data breach or emotion[al] distress can satisfy concreteness." *Medoff v. Minka Lighting, LLC,* No. 2:22-CV-08885-SVW-PVC, 2023 WL 4291973, at *4 (C.D. Cal. May 8, 2023) (collecting cases). These additional harms "can only qualify as concrete injuries in fact when they are based on a risk of harm that is either 'certainly impending' or 'substantial.'" *Id.* (quoting *I.C. v. Zynga, Inc.* 600 F. Supp. 3d 1034, 1052 (N.D. Cal. 2022).

TransUnion appears consistent with prior case law in this Circuit holding that theft of personal identifying information is sufficient to establish injury in fact. *Abdulaziz v. Twitter, Inc.*, No. 21-16195, 2024 WL 4688893, at *1 (9th Cir. Nov. 6, 2024) (citing *Zappos*, 888 F.3d at 1027; *Krottner*, 628 F.3d at 1140, 1143). In *Krottner*, Starbucks employees brought a putative class action against Starbucks after a laptop containing "the unencrypted names, addresses, and social security numbers of approximately 97,000 Starbucks employees" was stolen. 628 F.3d at 1140. The Ninth Circuit held that plaintiffs had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data." *Id.* at 1143.

Several years later, the Ninth Circuit reaffirmed *Krottner* in *Zappos*. In the intervening period, the Supreme Court had decided *Clapper v. Amnesty Int'l USA*,

568 U.S. 398, 416 (2013), raising the question of whether *Krottner* remained good law. 888 F.3d at 1025. In *Zappos*, plaintiffs sued after hackers breached the server of an online retailer. 888 F. 3d at 1023. The hackers allegedly stole the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information of over 24 million Zappos customers. *Id.* The Ninth Circuit rejected Zappos's argument that *Krottner* was no longer good law and held that plaintiffs sufficiently alleged standing based on risk of identity theft. *Id.* The court found that "[t]he sensitivity of the stolen data in this case [was] sufficiently similar to that in *Krottner* to require the same conclusion." *Id.* at 1027.

Following *Krottner* and *Zappos*, district courts in the Ninth Circuit have focused on the nature of the information that was stolen in determining whether a plaintiff faces an imminent risk of harm. *Medoff*, 2023 WL 4291973, at *5 (collecting cases); *see also In re Sequoia Benefits & Ins. Data Breach Litig.,* No. 22-CV-08217-RFL, 2024 WL 1091195, at *1 (N.D. Cal. Feb. 22, 2024). The Ninth Circuit has followed this approach since *TransUnion*, albeit in unpublished opinions, suggesting that *Krottner* and *Zappos* remain good law. *See Abdulaziz,* 2024 WL 4688893, at *1; *Greenstein v. Noblr Reciprocal Exch.*, No. 22-17023, 2024 WL 3886977, at *1 (9th Cir. Aug. 21, 2024) (distinguishing from *Krottner* and *Zappos* on the facts because plaintiffs failed to allege that their driver's license numbers were stolen).

Here, Plaintiffs allege that highly sensitive PII, including driver's license numbers and social security numbers, were stolen during the breach. (ECF No. 81 at ¶¶ 227, 233, 229.) Unlike the subset of plaintiffs in *TransUnion* whose reports were not disseminated, Plaintiffs' personal information here is already in the hands of hackers. Plaintiffs allege that this PII has already been found on the dark web and, in some cases, already been misused for fraud. (*Id.* at ¶¶ 271,

273.) Drawing all reasonable inferences in Plaintiffs' favor, these allegations plausibly allege that they face a substantial and imminent risk of identity theft. *See Medoff*, 2023 WL 4291973, at *6 (allegations that plaintiff's name and social security number were published on the dark web after hackers accessed the information through defendant's computer systems sufficient to allege injury in fact); *Greenstein v. Noblr Reciprocal Exch.*, 585 F. Supp. 3d 1220, 1227 (N.D. Cal. 2022) ("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"). The concrete harm that Plaintiffs have suffered in this case is akin to the harm suffered by the group of plaintiffs in *TransUnion* whose credit reports were actually disseminated to third parties.

Accordingly, the Court finds that Plaintiffs have sufficiently alleged a concrete and imminent threat of future harm sufficient to establish Article III injury in fact at the pleadings stage.

ii. Actual or Attempted Fraud

Some of the named Plaintiffs allege fraud, attempted fraud, identity theft, and misuse of PII. Plaintiff Gedwill alleges that he experienced a phishing attempt during which a stranger sent him money and requested that he return it. (ECF No. 81 at ¶ 71–72.) Caesars argues that this allegation is implausible because "[a] stranger would not need [] Gedwill's social security number, for instance, in order to send him money." (ECF No. 91 at 22.) This argument may be appropriate at summary judgment but does not support a facial challenge to standing at the motion to dismiss stage. *See Zappos*, 888 F.3d at 1028.

iii. Loss of Value of PII

Plaintiffs also allege injury in the form of loss of value and control over their PII. (ECF No. 81 at ¶¶ 18, 29, 50, 235–37, 276–85.) Plaintiffs allege that a "robust

market exists for stolen PII, which is sold and distributed on the dark web and through illicit criminal networks at specific, identifiable prices." (*Id.* at ¶ 277.) Plaintiffs allege that "[a] consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud," for example when they are denied credit or unable to open an electronic account. (*Id.* at ¶ 284.) Consumers also lose their ability to "negotiate sharing their PII for services" and are therefore deprived of that negotiated value. (*Id.* at ¶ 285.)

A court in this district recently upheld diminution in the value of PII as a cognizable theory of damages sufficient to survive a motion to dismiss where plaintiffs alleged "details about the existence of an economic market for selling stolen PII, including the fact that PII can be bought and sold at identifiable prices on established markets." *Smallman v. MGM Resorts Int'l*, 638 F. Supp. 3d 1175, 1191 (D. Nev. 2022). Defendants argue that Plaintiffs must allege both the existence of a market for their personal information and an impairment of their ability to participate in that market, citing *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1234 (D. Nev. 2020), *aff'd,* 845 F. App'x 613 (9th Cir. 2021). But *Smallman* and other district courts have rejected *Pruchnicki*'s formulation of the test as unsupported by Ninth Circuit precedent. *Smallman*, 638 F. Supp. 3d at 1190 (collecting cases).

The Court declines to adopt Defendants' interpretation of the pleading requirements. Plaintiffs have plausibly alleged injury in the form of diminution in value of PII by alleging the existence of a market for their stolen personal information and need not also allege an impairment of their ability to participate in that market. *See Smallman*, 638 F. Supp. 3d at 1191.

iv. Overpayment Theory

Plaintiffs allege that they suffered injury when they "overpaid for Caesars' services that should have been—but were not—accompanied by adequate data

security." (ECF No. 81 at ¶ 287.) Plaintiffs allege that, had they known about Caesars' deficient data security practices, "they would not have stayed at Caesars properties or would have paid less than they did for their rooms." (*Id.* at ¶ 290.) Caesars argues that this theory fails because only six of the named Plaintiffs are alleged to have stayed in Caesars' hotels and the remainder participated in a free rewards program. (ECF No. 91 at 24.) Caesars also argues that Plaintiffs are required to demonstrate that the price incorporated a particular sum that was understood by both parties to be allocated towards the protection on customer data. (*Id.*)

Plaintiffs point to *Smallman*, where the court acknowledged that "courts are divided on the level of detailed factual allegation required to show that data security was part of the bargain" but found more persuasive "the line of cases that accept at the pleading stage more general factual allegations about the plaintiff's expectations for data security and the contours of the parties' bargain." 638 F. Supp. 3d at 1190 (citing *In re Intel Corp. CPU Marketing, Sales Practices and Products Liability Litigation*, No. 3:18-2828, 2020 WL 1495304, at *8 (D. Or. Mar. 27, 2020)). Following *Smallman*, this Court considers, but does not find persuasive, cases that "requir[e] allegations of a particular sum of the purchase price being explicitly allocated for data security." *Id.* (internal quotation marks and citation omitted).

Plaintiffs do not respond to Caesars' argument that only six of the named Plaintiffs are alleged to have paid for a room at Caesars. And both cases Plaintiffs rely upon, *Bowen v. Energizer Holdings, Inc.*, 118 F.4th 1134, 1145 (9th Cir. 2024) and *Smallman*, 638 F. Supp. 3d at 1189–90, involved allegations of payments for products (as opposed to participation in free rewards programs). The Court finds that only those Plaintiffs who allege that they paid for Caesars' hotel rooms, and not those who merely signed up for the free rewards program, have alleged injury

in fact under this theory of harm.

v. Mitigation Efforts

Caesars argues that Plaintiffs cannot establish injury based on out-of-pocket costs or time spent on mitigation because to do so would be to "manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." (ECF No. 91 at 21 (citing *Clapper*, 568 U.S. at 416)). But as courts have found in other data breach lawsuits, "because the risk of harm here is a sufficient injury, the allegations of mitigation injuries made by these Plaintiffs are also sufficient." *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1263 (11th Cir. 2021); *see also In re Yahoo! Inc. Customer Data Sec. Breach Litig.,* No. 16-MD-02752-LHK, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017) (allegations of out-of-pocket mitigation expenses, including payment for credit monitoring services, sufficient to allege injury arising from data breaches); *In re Adobe Sys., Inc. Priv. Litig.,* 66 F. Supp. 3d 1197, 1217 (N.D. Cal. 2014) (costs incurred to mitigate future identity theft sufficient to establish injury in fact).

2. Traceability

Caesars next (briefly) contends that Plaintiffs cannot establish Article III standing because Plaintiffs' injuries are not "fairly traceable" to the data breach. (ECF No. 91 at 20–22.)

To establish traceability, "there must be a causal connection between the injury and the conduct complained of—the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court." *Lujan*, 504 U.S. at 560. "Proximate causation is not a requirement of Article III standing, which requires only that the plaintiff's injury be fairly traceable to the defendant's conduct." *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 134 (2014).

Plaintiffs allege that, after the breach, their information was misused or exploited to commit fraud. (ECF No. 81 at ¶¶ 271, 273.) Caesars' argument that Plaintiffs must allege that the breach included credit card or banking information to be traceable to fraud attempts is unpersuasive. Given the scope and sensitivity of the stolen PII (social security and driver's license numbers), it is reasonable to infer that such information could plausibly have been used to commit the fraud and other injuries that Plaintiffs allege. *See In re Sequoia*, 2024 WL 1091195, at *2 (plaintiffs sufficiently alleged that fraud was traceable to data breach that exposed sensitive data, though not banking or credit card information); *see also In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 467 (D. Md. 2020) (injuries of fraudulent charges on personal checking account and opening of "accounts for credit cards, consolidated loans, consumer accounts, and other lines of credit" were fairly traceable to data breach, even where no social security numbers or banking information was accessed).

B. Standing for Injunctive Relief

Caesars next challenges Plaintiffs' standing to seek injunctive relief, arguing that they cannot show a threat of repeated injury and again pointing to *TransUnion*. (ECF No. 91 at 26.) Plaintiffs respond that they are seeking injunctive relief to address the harms caused by Caesars' inadequate security protocols. (ECF No. 96 at 21.)

Plaintiffs allege that Caesars' inadequate security protocols remain in place today and that Caesars continues to hold their data. (ECF No. 81 at ¶¶ 304–305, 306.) These allegations are sufficient, at this stage in the proceedings, to demonstrate standing for injunctive relief. *See Baton v. Ledger SAS,* 740 F. Supp. 3d 847, 881 (N.D. Cal. 2024) (standing to seek injunctive relief as to inadequate security where plaintiffs alleged that they remain at imminent risk that further compromises of their personal information will occur in the future); *Stallone v.*

Farmers Group, Inc., No. 221CV01659GMNVCF, 2022 WL 10091489, at *9 (D. Nev. Oct. 15, 2022) (standing for injunctive relief where plaintiffs alleged that without injunctive relief, Plaintiff's PII could be "obtained again in the same unauthorized manner").

C. Damages for Common Law Claims

Caesars argues that Plaintiffs' common law claims fail because their alleged harms are too speculative, relying on the same arguments that it makes with regard to standing. (ECF No. 91 at 26–27.) Caesars primarily relies on its arguments regarding injury in fact, and only specifically challenges (as an example) mitigation expenses. But courts in this Circuit have acknowledged that, at the motion to dismiss stage, allegations of lost time are plausible allegations of damages. *Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 918 (S.D. Cal. 2020); *see also In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F. Supp. 3d 1284, 1296 (S.D. Cal. 2020) ("[i]ncreased time spent monitoring one's credit and other tasks associated with responding to a data breach have been found by other courts to be specific, concrete, and non-speculative").

At this early stage of litigation, Plaintiffs allege plausible damages in the form of actual and attempted fraud and identity theft, loss of value of PII, and lost time.

D. Negligence

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.*, 221 P.3d 1276, 1280 (Nev. 2009). Caesars argues that Plaintiffs do not adequately allege duty, breach, or damages. (ECF No. 91 at 27–34.)

1. Duty

Caesars argues that it had no duty to protect Plaintiffs' PII "from being exposed to cybercriminals." (ECF No. 91 at 27.) This is not an accurate description of Plaintiffs' allegations. Plaintiffs contend that Caesars owed Plaintiffs a duty "to protect their PII once Caesars collected it." (ECF No. 96 at 22.) Plaintiffs allege that Caesars had "a duty to exercise reasonable care in safeguarding, securing, and protecting Class Members' PII." (ECF No. 81 at ¶ 328.) Plaintiffs allege that Caesars' duty arose from, among other things, the special relationship between Caesars and its customers, the FTC Act, state law, industry standards, and representations made to Plaintiffs. (*Id.* at ¶ 219.)

District courts have found comparable allegations sufficient to survive motions to dismiss negligence claims. *See, e.g., Smallman*, 638 F. Supp. 3d at 1188 (defendant breached duty of care in manner of collecting, maintaining, and controlling customers' sensitive personal and financial information); *In re Accellion, Inc. Data Breach Litig.*, 713 F. Supp. 3d 623, 634 (N.D. Cal. 2024), *reconsideration denied*, No. 21-CV-01155-EJD, 2024 WL 4592367 (N.D. Cal. Oct. 28, 2024) (California recognizes a duty by companies to take reasonable steps to protect all sensitive information they obtain from individuals); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1325 (N.D. Ga. 2019) (duty of care to safeguard personal information in its custody where defendants "knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures"); *Stasi*, 501 F. Supp. 3d at 914 (collecting cases).

Plaintiffs have adequately alleged that the risk of harm was foreseeable. They allege that, just months before the data breach, Caesars told investors that cyberattacks were a significant risk factor. (ECF No. 81 at ¶ 250.) They allege that Caesars was aware that several of its competitors had experienced data breaches in recent years, and that as many as 15 to 20 percent of data breaches occur

within the hospitality industry. (*Id.* at ¶¶ 244–45.) Accordingly, at this stage in the proceedings, Plaintiffs plausibly allege duty.

Caesars also argues that Plaintiffs' claim for negligence *per se* does not supply duty. (ECF No. 91 at 29–30.) Because Plaintiffs have adequately alleged duty and because Caesars does not move to dismiss the negligence *per se* claim, the Court does not address this argument.

2. Breach

Caesars argues that Plaintiffs have not alleged breach because they have not specified exactly how Caesars' data security measures were inadequate. (ECF No. 91 at 30–31.) Plaintiffs allege that Caesars retained their PII for longer than necessary, thus failing to adhere to standard purging and data minimization processes. (ECF No. 81 at ¶¶ 396, 253.) Plaintiffs allege that Caesars "intentionally failed to encrypt the PII while it was store on Caesars' server." (*Id.* at ¶ 430.) And Plaintiffs allege that Caesars allowed an intruder to download the PII five days after it noticed the suspicious activity. (*Id.* at ¶ 225.) At this stage of the proceedings, Plaintiffs have sufficiently alleged that Caesars breached the duty of care owed to them. *See Smallman*, 638 F. Supp. 3d at 1188.

3. Economic Loss Doctrine

Caesars argues that Plaintiffs' damages are barred by the economic loss doctrine. (ECF No. 91 at 31–32.) Plaintiffs argue that the economic loss doctrine is not applicable because they allege non-economic damages, because Caesars' duty is based on statutory obligations, and because a special relationship exists. (ECF No. 96 at 25.)

"Under the economic loss doctrine 'there can be no recovery in tort for purely economic losses.'" *Urban Outfitters, Inc. v. Dermody Operating Co., LLC*, 572 F. Supp. 3d 977, 995 (D. Nev. 2021) (quoting *Calloway v. City of Reno*, 993 P.2d 1259, 1263 (Nev. 2000)). But "[i]n the data breach context, courts within the

Ninth Circuit have found that an individual's loss of control over the use of their identity due to a data breach and the accompanying impairment in value of PII constitutes non-economic harms." *Smallman*, 638 F. Supp. 3d at 1188 (collecting cases).

Plaintiffs have alleged loss of control over use of their identity, loss of time, and imminent risk of identity theft, all of which are non-economic harms. Accordingly, the economic loss doctrine does not bar Plaintiffs' negligence claims.

E. Implied Contract

Caesars argues that Plaintiffs' claim for breach of implied contract fails because Plaintiffs have not pled the existence of an implied contract, breach, or damages. (ECF No. 91 at 32–33.) Specifically, Caesars argues that Plaintiffs fail to identity any specific promise that was allegedly breached and fail to explain how the promise was breached. (*Id.*) Plaintiffs argue that the existence of an implied contract is a question of fact that the Court should decline to address on a Rule 12(b)(6) motion. (ECF No. 96 at 28–30.)

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. *Saini v. Int'l Game Tech.*, 434 F. Supp. 2d 913, 919–20 (D. Nev. 2006) (citing *Richardson v. Jones*, 1 Nev. 405 (Nev. 1865)). Although the terms of an implied contract are manifested by conduct rather than written words as in an express contract, both "are founded upon an ascertainable agreement." *Smith v. Recrion Corp.*, 541 P.2d 663, 664–65 (Nev. 1975).

At this stage, Plaintiffs have adequately stated a claim for breach of implied contract. Plaintiffs allege that Caesars required that Plaintiffs provide their PII to participate in the rewards program. (ECF No. 81 at ¶ 4.) Plaintiffs allege that they provided their PII to Caesars with the understanding that Caesars would take adequate data security measures. (*Id.* at ¶ 214.) Plaintiffs allege that this mutual

understanding was based in part on Caesars' privacy policy, which stated that Caesars "maintain[s] physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under [their] control." (*Id.* at ¶ 215–16.) As to breach, Plaintiffs allege that Caesars did not take adequate data security measures. And for the reasons set forth above, *supra* Part III.C, Plaintiffs have adequately alleged damages. Accordingly, the Court denies Caesars' motion to dismiss the implied contract claim.

F. Unjust Enrichment

Caesars argues that Plaintiffs' unjust enrichment claim fails for two reasons. First, Caesars contends that Plaintiffs cannot pursue equitable remedies without showing that they lack an adequate remedy at law. (ECF No. 91 at 34–35.) Second, Caesars contends that Plaintiffs fail to plead that they conferred any benefit on Caesars, arguing that PII does not have any independent monetary value. (*Id.*) Plaintiffs respond that they do not have an adequate remedy at law because Caesars retains their information and because they are seeking injunctive relief requiring Caesars to improve its data security systems. (ECF No. 96 at 30–31.) Plaintiffs also point to their allegations that PII has independent monetary value. (*Id.*)

In Nevada, the elements of an unjust enrichment claim are: "a benefit conferred on the defendant by the plaintiff, appreciation by the defendant of such benefit, and acceptance and retention by the defendant under circumstances such that it would be inequitable for him to retain the benefit without payment of the value thereof." *Leasepartners Corp. v. Robert L. Brooks Tr. Dated Nov. 12, 1975*, 942 P.2d 182, 187 (Nev. 1997). "An action based on a theory of unjust enrichment is not available when there is an express, written contract, because no agreement can be implied when there is an express agreement." *Id.*

Plaintiffs allege that they conferred a benefit on Caesars in the form of their valuable PII and that Caesars appreciated that benefit without employing adequate data security measures. (ECF No. 81 at ¶¶ 357–68.) Plaintiffs allege that they have no adequate remedy at law because Caesars retains their PII, exposing Plaintiffs to a risk of future data breaches. (*Id.* at ¶ 366.) *Cf Smallman*, 638 F. Supp. 3d at 1198 (dismissing plaintiffs' unjust enrichment claim because plaintiffs did not allege lack of adequate remedy at law). And Plaintiffs allege that PII has independent monetary value, as discussed above. *See supra* Part III.A.1.iii.

Accordingly, the Court denies Caesars' motion to dismiss Plaintiffs' unjust enrichment claim.

G. Statutory Claims

Caesars argues that Plaintiffs' consumer protection claims fail because they are insufficiently pled under Rule 9(b), and that Plaintiffs' data breach notification statute claims fail because they do not allege cognizable harm. (ECF No. 91 at 35–41.) Caesars separately challenges several individual statutory claims. (*Id.* at 41–53.)

1. Consumer Protection Claims

Caesars argues that Plaintiffs' consumer protection (or "misrepresentation-based") claims (Counts IV, V, VI, IX, X, XI, XII, XIII, XV, XVI, XVIII) should be dismissed for failure to comply with Rule 9(b)'s heightened pleading standard. (ECF No. 91 at 35–41.) Plaintiffs contend that Rule 9(b) does not apply because Plaintiffs allege only negligence-based or reckless conduct, and in the alternative that Plaintiffs have met Rule 9(b) pleading requirements. (ECF No. 96 at 31–33.) Plaintiffs also argue that Caesars' tactic of arguing in the aggregate "elides important distinctions between the statutes [and] their varying pleading requirements." (ECF No. 96 at 31.) The Court agrees.

Assuming but not deciding that Rule 9(b) applies to all nine statutes, Plaintiffs' allegations meet the particularity requirements of Rule 9(b). Plaintiffs allege that Caesars knew its data security practices were deficient (ECF No. 81 at ¶¶ 252–68), that Caesars knew the hotel industry is a frequent target of cyberattacks (*Id.* at ¶¶ 243–51), and that Caesars failed to disclose its deficient management of PII (*Id.* at ¶¶ 239-42). Plaintiffs sufficiently allege that Caesars' failure to disclose its data security deficiencies to Plaintiffs constitutes a knowing omission. *See Smallman,* 638 F. Supp. 3d at 1200.

Accordingly, the Court denies Caesars' motion dismiss Plaintiffs' consumer protection claims.

2. Data Breach Notification Statute Claims

Caesars argues that Plaintiffs' data breach notification statutes claims (Counts VII, VIII, and XVII) should be dismissed for failure to allege unreasonable delay or harm caused by the delay. (ECF No. 91 at 40–41.) Plaintiffs argue that they sufficiently allege cognizable and incremental harm. (ECF No. 96 at 33–34.)

The California, Illinois, and Virginia data breach notification statutes require companies to notify individuals of data breaches without unreasonable delay. *See In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1149 (C.D. Cal. 2021) (the CCRA requires businesses doing business in California to make disclosure of data breaches "in the most expedient time possible and without unreasonable delay") (quoting Cal. Civ. Code § 1798.82); 815 Ill. Comp. Stat. 530/10(a) (businesses must provide a "disclosure notification … in the most expedient time possible and without unreasonable delay"); Va. Code. § 18.2-186.6(B) (notice of the data breach must occur "without unreasonable delay").

Plaintiffs allege that Caesars' nearly two-week delay in notifying states' attorneys' generals and in sending individual notices "exacerbated harm to Class Members by preventing them from taking steps to mitigate Caesars failures and

trying to protect themselves." (ECF No. 81 at ¶ 230.) Plaintiffs also allege that Caesars still has not disclosed several important facts, including how many rewards program members were affected by the breach, what information was taken, and what steps Caesars has taken to ensure that such an attack does not happen again. (*Id.* at ¶ 232.)

Courts have found such allegations sufficient under the California, Illinois, and Virginia timely disclosure statutes. *See In re Solara*, 613 F. Supp. 3d at 1300 (plaintiffs adequately alleged incremental harm under California Consumer Records Act as a result of delay where five-month delay prevented them from taking steps to protect personal information); *In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 590 (N.D. Ill. 2022) (denying motion to dismiss claims under Illinois and California data notification statutes because allegations of post-remedial actions and harm from the breach make it "plausible to conclude that Defendants' more timely disclosure would have prevented additional incremental injury"); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 417 (E.D. Va. 2020) ("additional monitoring costs" plausibly fall within the scope of the Virginia Personal Information Breach Notification Act).

Accordingly, the Court denies Caesars' motion to dismiss Plaintiffs' data breach notification statute claims.

3. Texas Deceptive Practices Act

Caesars argues that Plaintiff Huddleston did not comply with the Texas Deceptive Practices Act's ("DTPA") pre-suit written notice requirements because notice was given too late and did not provide sufficient detail. (ECF No. 91 at 41–42.) Under the DTPA, a plaintiff must give written notice at least 60 days before filing suit "advising the person in reasonable detail of the consumer's specific complaint and the amount of economic damages . . . ." Tex. Bus. & Com. Code Ann. § 17.505. Here, Plaintiffs provided written notice of the lawsuit

approximately thirty days before filing the Consolidated Class Action Complaint. (ECF No. 96-1.) The letter noted that counsel was already aware of the allegations from previously filed complaints and that it was providing the letter as "additional notice." (*Id.* at 4.) Those complaints were filed more than 90 days before the Consolidated Class Action Complaint. (ECF No. 81 at ¶ 560.)

"The notice requirement is intended to give the defendant an opportunity to make a settlement offer and minimize litigation expense." *Star Houston, Inc. v. Kundak*, 843 S.W.2d 294, 297 (Tex. App. 1992). Caesars has failed to show any harm from Huddleston's alleged technical violation of the sixty-day notice requirement. *See id.* The Court therefore declines to dismiss the TDPA claim or abate the lawsuit.

4. Nevada Consumer Fraud Act

Plaintiffs allege two violations of two subsections of NRS § 598 (the Nevada Deceptive Trade Practices Act ("NDTPA")) under their Nevada Consumer Fraud Act ("NCFA") claim. (ECF No. 81 at ¶¶369–381.) The NCFA provides that an action may be brought by any person who is a victim of consumer fraud, and defines "consumer fraud" to mean, among other things, "[a] deceptive trade practice as defined in NRS 598.0915 to 598.0925, inclusive." NRS 41.600(1)(e). Plaintiffs allege a violation of that statute under two definitions of "deceptive trade practice."

A person engages in a "deceptive trade practice" when they knowingly "fail[] to disclose a material fact in connection with the sale or lease of goods or services." NRS 598.0923(1)(b). (ECF No. 81 at ¶ 371.) Plaintiffs allege that Caesars violated this provision by failing to disclose the material fact that its data security practices were deficient and that its cloud server security settings were not adequate to protect consumers' PII. (*Id.* at ¶ 371.) Caesars argues that this claim fails because Plaintiffs did not allege a duty to disclose, relying on *Soffer v.*

Five Mile Cap. Partners, LLC, No. 2:12-CV-1407 JCM GWF, 2013 WL 638832 (D. Nev. Feb. 19, 2013) and *Taddeo v. Taddeo,* No. 2:08-CV-01463-KJD, 2011 WL 4074433, at *5 (D. Nev. Sept. 13, 2011). But those cases involved claims for common law fraud, not statutory fraud, and "[s]tatutory offenses that sound in fraud are separate and distinct from common law fraud." *Betsinger v. D.R. Horton, Inc.,* 232 P.3d 433, 436 (Nev. 2010); *see Smallman*, 638 F. Supp. 3d at 1199. Caesars has therefore failed to show that Plaintiffs are required to demonstrate that Caesars had a duty to disclose.

A deceptive trade practice also includes knowingly "violat[ing] a state or federal statute or regulation relating to the sale or lease of goods or services." NRS 598.0923(1)(c). Plaintiffs allege that Caesars violated this provision by breaching several federal and state statutes, including NRS 603A.210(1), which requires that "[a] data collector that maintains records which contain personal information of a resident of this States shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure." NRS 603A.210(1). Caesars argues that Plaintiffs must plead with particularity how the facts of this case pertain to that specific statute, but the only case it relies upon for that proposition, *Baba v. Hewlett-Packard Company,* discusses California's UCL. No. C 09-05946 RS, 2010 WL 2486353, at *6 (N.D. Cal. June 16, 2010). Caesars does not cite to any Nevada law requiring such specificity at the pleading stage. The NDTPA is a "remedial statutory scheme" which is afforded a "liberal construction." *Yip v. Bank of Am., N.A.*, No. 2:21-CV-01254-ART-EJY, 2024 WL 3742910, at *12 (D. Nev. Aug. 9, 2024) (citing *Poole v. Nevada Auto Dealership Invs., LLC*, 449 P.3d 479, 485 (Nev. App. 2019) and *R.J. Reynolds Tobacco Co. v. Eighth Jud. Dist. Ct. in & for Cnty. of Clark*, 514 P.3d 425, 430 (Nev. 2022)). Plaintiffs allege that Caesars is a data collector that maintains records of in-state residents, and that it failed to

implement reasonable security measures. The Court therefore denies Caesars' motion to dismiss on this ground.

Plaintiffs also allege that Caesars' violation of the FTC Act constitutes a violation of the NDTPA under NRS 598.0923(1)(c). (ECF No. 81 at ¶ 375.) Caesars argues again that this allegation is not specific enough. For the same reasons, the Court denies Caesars' motion to dismiss on this ground.

5. California Statutory Claims

Caesars argues that California Plaintiffs' claims under California's Unfair Competition Law ("UCL") and the Consumer Legal Remedies Act ("CLRA") fail for lack of statutory standing and failure to state a claim.

i. Standing

Caesars contends that Plaintiffs lack standing under the UCL and CLRA because Plaintiffs fail to allege "lost money or property" (as required for the UCL) or "economic injury" (as required for the CLRA). (ECF No. 91 at 44–45.)

To satisfy the statutory standing requirement under the UCL, a plaintiff must merely suffer an injury in fact that is an "economic injury." *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021) (citing *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 321–22, (2011)). "[A]ny plaintiff who has standing under the UCL's . . . 'lost money or property' requirement will, *a fortiori,* have suffered 'any damage' for purposes of establishing CLRA standing." *Hinojos v. Kohl's Corp.*, 718 F.3d 1098, 1108 (9th Cir. 2013), *as amended on denial of reh'g and reh'g en banc* (July 8, 2013).

Plaintiffs point to allegations of loss of value of PII, benefit of the bargain damages, including overpayment for hotel rooms, out-of-pocket costs in mitigation efforts, and the purchase of identity protection services. (ECF No. 96 at 37–38.) These allegations are sufficient to establish standing under the UCL and CLRA. *See Smallman*, 638 F. Supp. 3d at 1202 (allegations that plaintiffs

paid more for hotel rooms as a result of defendant's omissions regarding data security policies sufficient to establish standing under the UCL); *In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1219 (C.D. Cal. 2017) (allegations that plaintiffs would have paid less for products had defendant properly disclosed its consumer data collection and disclosure practices cognizable under UCL and CLRA); *In re Yahoo! Inc.*, 2017 WL 3727318, at *21 (benefit of the bargain losses sufficient to allege standing under the UCL); *Calhoun*, 526 F. Supp. 3d at 636 (loss of personal information is economic injury conferring standing under the UCL).

ii. UCL

Caesars argues that Plaintiffs have failed to allege reliance, which is required for claims under the fraud prong of the UCL. (ECF No. 91 at 45–46); *In re Tobacco II Cases*, 207 P.3d 20, 39 (Cal. 2009).

"[A]t the motion to dismiss stage, actual reliance . . . is inferred from the misrepresentation of a material fact." *Moore v. Mars Petcare US, Inc.*, 966 F.3d 1007, 1021 (9th Cir. 2020). "Whether a misrepresentation is sufficiently material to allow for an inference of reliance is generally a question of fact that cannot be decided at the motion to dismiss stage." *Id.* Plaintiffs allege that Caesars neglected specific data security practices, explain what Caesars should have done, and allege that Caesars misrepresented that it would protect Plaintiffs' PII. (ECF No. 81 at ¶¶ 394, 395, 398–404.) These allegations are sufficient to survive a motion to dismiss.

The Court similarly rejects Caesars' argument that Plaintiffs have failed to show unlawful, unfair, or fraudulent conduct as premature. *See Broomfield v. Craft Brew All., Inc.*, No. 17-CV-01027-BLF, 2017 WL 3838453, at *5 (N.D. Cal. Sept. 1, 2017) ("the deceptive nature of a business practice under California's consumer protection statutes is usually a question of fact that is inappropriate

for decision on . . . a motion to dismiss").

Caesars also argues that Plaintiffs' UCL claim should be dismissed because they do not plead that they lack an adequate remedy at law. (ECF No. 91 at 46.) The Court already considered and rejected this argument above. *See supra* Part III.F.

iii. CLRA

Caesars asserts that Plaintiffs' CLRA claim fails for the same reasons as the UCL claim. (ECF No. 91 at 48.) For the same reasons, the Court denies the motion to dismiss this claim.

6. Pennsylvania Unfair Trade Practice and Consumer Protection Law

Caesars argues that Plaintiffs Smith and Katz's claims under the Pennsylvania Unfair Trade Practice and Consumer Protection Law ("UTPCPL") should be dismissed for failure to establish any "ascertainable loss of money or property," as required under the UTPCPL. *Benner v. Bank of Am., N.A.*, 917 F. Supp. 2d 338, 359 (E.D. Pa. 2013); (ECF No. 91 at 48–49.) Both Plaintiffs allege loss of value of their PII (ECF No. 81 at ¶¶ 170, 179), "which serves as [a] form of lost property" under the UTPCPL." *Opris v. Sincera Reprod. Med.*, No. CV 21-3072, 2022 WL 1639417, at *13 (E.D. Pa. May 24, 2022). That is sufficient to survive a motion to dismiss.

7. Virginia Consumer Protection Act

Caesars argues that Plaintiff Lackey's Virginia Consumer Protection Act ("VCPA") claim should be dismissed, in addition to its generalized arguments about particularity, for failure to plead "actual damages," and because Lackey cannot bring the claim on behalf of a class. (ECF No. 91 at 49.)

First, the VCPA's loss requirement is "expansive" compared to other state consumer protection statutes. *In re Gen. Motors LLC Ignition Switch Litig.*, 339 F. Supp. 3d 262, 332 (S.D.N.Y. 2018); *Attias v. CareFirst, Inc.*, 518 F. Supp. 3d 43,

56 (D.D.C. 2021). Plaintiff Lackey pleads the loss of value of PII, benefit of the bargain damages, and mitigation efforts. (ECF No. 81 at ¶¶ 199, 200.) These allegations are sufficient at this stage.

Second, "[t]he question of whether a class action may be maintained with respect to the [VCPA] is proper to consider at the class certification stage rather than in considering a motion to dismiss." *Mouzon v. Radiancy, Inc.*, 200 F. Supp. 3d 83, 90 (D.D.C. 2016).

8. Minnesota Statutory Claims

Caesars argues that the Minnesota Plaintiffs fail to state a claim under the Minnesota Deceptive Trade Practices Act ("MDTPA") and Minnesota Consumer Fraud Act ("MCFA") because they do not allege deceptive or misleading practices in connection with the sale or advertisement of "merchandise." (ECF No. 91 at 50.) Plaintiffs point to the broad statutory definition of "merchandise," which includes, among other things, "services." (ECF No. 96 at 44); Minn. Stat. § 325F.68(2). To the extent that Caesars argues that "the only viable data breach class action lawsuits would be those asserting claims against companies that sell data security services," the Court agrees with Plaintiffs that "such an argument would be nonsensical. *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 772–73 (C.D. Ill. 2020).

Caesars argues that the MDTPA claim also fails because the MDTPA only permits injunctive relief. Plaintiffs have plausibly pled likelihood of future harm and seek injunctive relief, as addressed above. *Supra* Part III.B. Accordingly, the Court denies Caesars' motion to dismiss the Minnesota Plaintiffs' statutory claims.

9. Illinois Statutory Claims

Caesars argues that Plaintiffs' claims under the Illinois Deceptive Trade Practices Act ("IDTPA") and Illinois Consumer Fraud Act ("ICFA") fail for the same

reasons. (ECF No. 91 at 50.)

For the reasons set forth above, the Illinois Plaintiffs have plausibly pled likelihood of future harm based on Caesars' continued possession of their data. They have also alleged actual damages under ICFA based on loss of value of PII, mitigation efforts, and loss of time. And they have alleged that they received communication from Caesars. (ECF No. 81 at ¶¶ 236–37.) Accordingly, the Court denies Caesars' motion to dismiss the Illinois Plaintiffs' statutory claims.

10. New York General Business Law Claim

Caesars finally argues that the New York Plaintiffs' New York General Business Law ("GBL") claim should be dismissed for failure to identify a misleading representation or omission by Caesars. (ECF No. 91 at 52.)

Section 349 of the GBL prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service." N.Y. Gen. Bus. § 349(a). To state a GBL claim, the New York Plaintiffs must allege (1) that Caesars' "act or practice was consumer-oriented," (2) that the act or practice "was misleading in a material way," and (3) that plaintiff "suffered injury as a result of the deceptive act." *Stutman v. Chem. Bank*, 731 N.E.2d 608, 611 (N.Y. 2000). Caesars challenges only the second element. Plaintiffs have satisfied this element by alleging that Caesars misrepresented that it would protect their PII, and that Caesars failed to comply with statutory duties regarding the security and privacy of Plaintiffs' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45. *See Smallman*, 638 F. Supp. 3d at 1206 (declining to dismiss claims based on similar allegations); *In re Marriott Int'l, Inc.*, 440 F. Supp. 3d at 493 (duties imposed by the FTC Act serve as predicate for violations of the GBL). Accordingly, the Court denies Caesars' motion to dismiss Plaintiffs' GBL claim.

IV. CONCLUSION

The Court therefore DENIES Defendant's to dismiss (ECF No. 91).

The Court GRANTS Plaintiffs' motion for leave to file supplemental authorities (ECF No. 114).

DATED: August 15, 2025

ANNE R. TRAUM
UNITED STATES DISTRICT JUDGE