MEMORANDUM OF POINTS AND AUTHORITIES

Adversarial Review of the Operative Amended Complaint, Defendant's Motion to Dismiss, and Recommendations to Strengthen Plaintiff's Claims Before Opposition

Matter: *Huddleston v. Caesars Entertainment, Inc.*

Court: United States District Court for the District of Nevada

Case No.: 2:26-cv-01237-APG-EJY · Chief Judge Andrew P. Gordon · Magistrate Judge Elayna J. Youchah

Prepared for: Counsel for Plaintiff — Cohen Milstein Sellers & Toll PLLC

Date: August 13, 2026

Controlling Deadline

Plaintiff's opposition to Caesars Entertainment, Inc.'s Motion to Dismiss the Amended Complaint (ECF 011) is due September 4, 2026 (ECF 13). After adversarial testing of the alternatives, the settled sequence is: confirm Huddleston's 2026 notice status; amend the operative pleading to official primary sources and plaintiff-specific injury; then oppose. Opposition-only on the complaint is rejected as the working strategy. Every recommendation in this memorandum must be executed against that date.

TL/DR: *Amend first. The complaint's contact-and-DOB pleading is a standing trap. See Sections II(C) and III.*

I. INTRODUCTION AND SCOPE

This memorandum undertakes a full adversarial review of the operative Amended Class Action Complaint and Caesars' motion to dismiss in *Huddleston v. Caesars Entertainment, Inc.*, No. 2:26-cv-01237-APG-EJY (D. Nev.). The purpose is to identify material vulnerabilities so that counsel may cure those vulnerabilities before the September 4, 2026, opposition deadline.

Each of the following materials was reviewed in preparation of this memorandum: (1) the PACER Docket Report through ECF 13; (2) the Amended Class Action Complaint, ECF 004; and (3) Defendant's Motion to Dismiss the Amended Complaint, ECF 011. Related-case materials from Ceasars Entertainment's 2023 data breach litigation.[1]

External and official sources reviewed include Massachusetts and Washington Attorney General 2026 notice materials; the May 19, 2026 Caesars consumer notice template; Washington AG directory categories; SEC EDGAR materials including the September 14, 2023 Form 8-K and the March 31, 2026 Form 10-Q; Caesars' CSR Position on Data Privacy & Security (last updated September 2022) and 2025 CSR Appendix; and official primary opinions including *TransUnion LLC v. Ramirez*, *In re Zappos.com, Inc.*, *Popa v. Microsoft Corp.*, *Kisil v. Illuminate Education, Inc.*, *Greenstein v. Noblr Reciprocal Exchange*, and *Abdulaziz v. Twitter, Inc.*. Current Nevada Revised Statutes text for NRS 603A.040, 603A.210, and 598.0923 was reviewed.

Technology-aided record indexing

Technology-aided indexing was used to extract and inventory filed documents and collateral materials. The index, however, was not a substitute for reading the enumerated filings and official sources. Dispositive standing authorities were verified through official court PDFs and CourtListener where available.

[1] *In re Data Breach Security Litigation Against Caesars Entertainment, Inc.*, No. 2:23-cv-01447-ART-BNW (D. Nev.) (Traum, J.; Weksler, M.J.).

II. GOVERNING LAW AND PROCEDURAL POSTURE

A. Jurisdiction, parties, and the September 4 deadline

This is an early putative class action. Plaintiff Mark Huddleston, pled as a Texas resident and Caesars Rewards member since 2007, filed the original and amended complaints on April 22, 2026. Subject-matter jurisdiction is pled under CAFA, 28 U.S.C. § 1332(d), though the docket currently codes the case as federal-question negligence. After waiver of service and an extension, Caesars filed to dismiss (ECF 011), invoking Rules 12(b)(1), 12(b)(6), and 9(b), and requesting dismissal with prejudice. The Court deferred Local Rule IA 11-2 verified petitions pending a motion to consolidate.

B. Article III standing after TransUnion

Caesars centers *TransUnion LLC v. Ramirez*[2] for the proposition that a risk of future harm alone does not confer Article III standing for damages, and argues that contact information and dates of birth cannot support an imminent identity-theft theory. That framing is the stronger reading of the current operative complaint. Damages standing and injunctive standing must be analyzed as distinct theories. Injunctive standing based on ongoing retention is a secondary argument after amendment, not a substitute for repairing damages standing.

The published Ninth Circuit decisions in *In re Zappos.com, Inc.*[3] and *Krottner v. Starbucks Corp.*[4] still supply the plaintiff-side architecture for substantial-risk standing when highly sensitive personal information is stolen. An unpublished November 6, 2024 memorandum in *Abdulaziz v. Twitter, Inc.*[5] reaffirmed that theft of personal identifying information can establish injury in fact, citing *Zappos* and *Krottner*. That line supports amendment to high-sensitivity, plaintiff-specific facts. It does not salvage the complaint as written.

Recent Ninth Circuit dispositions sharpen the defense trap. An unpublished September 8, 2025 memorandum in *Kisil v. Illuminate Education, Inc.*[6] affirmed dismissal where plaintiffs alleged no actual identity theft, the compromised data was not Social Security or financial information, and nothing had been released. An unpublished August 21, 2024 memorandum in *Greenstein v. Noblr Reciprocal Exchange*[7] held that a notice saying information "may have been accessed" does not plead that the named plaintiff's data was stolen. The published August 26, 2025 opinion in *Popa v. Microsoft Corp.*[8] applies *TransUnion*'s common-law-analogue requirement to state claims and rejects a free-roaming privacy injury. Unpublished Ninth Circuit memoranda are not precedent except as provided by Ninth Circuit Rule 36-3; they are included because defense counsel is expected to cite them against the current pleading.

C. Two findings that reframe strategy

Two verified propositions should drive every strategic decision that follows.

---

[2] *TransUnion LLC v. Ramirez*, 594 U.S. 413, 141 S. Ct. 2190, 210 L. Ed. 2d 568 (2021).
[3] *In re Zappos.com, Inc.*, 888 F.3d 1020 (9th Cir. 2018) (also reported as *Stevens v. Zappos.com, Inc. (In re Zappos.com, Inc.*), 888 F.3d 1020 (9th Cir. 2018)).
[4] *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010).
[5] *Abdulaziz v. Twitter, Inc.*, No. 21-16195 (9th Cir. Nov. 6, 2024) (unpublished memorandum) (D.C. No. 3:19-cv-06694-LB (N.D. Cal.)).
[6] *Kisil v. Illuminate Education, Inc.*, No. 23-4114, 2025 WL 2589000 (9th Cir. Sept. 8, 2025) (unpublished memorandum).
[7] *Greenstein v. Noblr Reciprocal Exchange*, No. 22-17023, 2024 WL 3886977 (9th Cir. Aug. 21, 2024) (unpublished memorandum) (D.C. No. 4:21-cv-04537-JSW (N.D. Cal.)).
[8] *Popa v. Microsoft Corp.*, 153 F.4th 784 (9th Cir. 2025) (No. 24-14; D.C. No. 2:23-cv-00294-JLR (W.D. Wash.); filed Aug. 26, 2025) (also cited as 2025 WL 2448824).

1. Contact-and-DOB-only pleading is not a viable primary standing theory. Opposing dismissal on the operative complaint alone is unlikely to succeed. The related Traum denial (in the 2023 Caesars case) suggests that the complaint in this matter would do well to focus on high-sensitivity, plaintiff-specific facts. Use Traum persuasively after amendment, if the 2026 facts look like the 2023 facts.

2. Nevada statutory predicates on the current complaint are mismatched. Official current NRS 603A.210(1) reaches personal information of a resident of this State, and NRS 603A.040's definition of personal information requires a name combined with enumerated sensitive elements such as a Social Security number or driver's license number—not name plus date of birth or contact information alone. Official current NRS 598.0923 places knowing failure to disclose and knowing statutory violation in subsections (1)(b) and (1)(c). ECF 004's citations to subsections (2) and (3) for those predicates do not match the current statute and must be corrected.

The case should therefore be rebuilt around two pillars:

(1) a Rule 15 amended complaint keyed to official February 23 / May 19 notices, Huddleston-specific inclusion and data elements, and concrete 2026 injury; and

(2) a claim structure that prunes NRS 603A as a predicate for this Texas plaintiff unless a Nevada named plaintiff is added, and that rebuilds any NCFA count only on corrected statutory text.

III. EXECUTIVE SUMMARY

Official Attorney General consumer notices confirm that on February 23, 2026, Caesars identified suspicious activity in certain cloud-hosted platforms used to store data, and that Caesars mailed consumer notices dated May 19, 2026. The Washington Attorney General directory lists compromised-information categories including Social Security numbers, driver's license or state ID numbers, dates of birth, and passport numbers for that filing. The problem is that the operative Amended Complaint does not use that record.

That public-record backbone is helpful and should be included. As a litigation vehicle, however, the current complaint contains potential weaknesses. The principal vulnerabilities, in order of importance, are as follows.

1. Plaintiff has self-limited standing. The complaint alleges only contact information and dates of birth, cites a Gambling News article titled "Social Media Rumors" as the sole contemporaneous 2026 source, and does not allege receipt of a consumer notice letter, enumerated data elements unique to Huddleston, out-of-pocket mitigation costs, or a concrete 2026 misuse event. Defense will lock the Court into that ceiling.

2. The class is keyed to a March 2026 "discovery" that is impeachable against February 23 and May 19 official notices and an April 22 filing date. Counsel marketing that uses a March 1 date or "tens of millions" is not a pleading source.

3. If Huddleston is not in the 2026 notice set, amendment cannot manufacture standing for him. Continuity as a 2023 named plaintiff and Rewards tenure since 2007 are weaker substitutes for 2026 exposure. Confirm inclusion promptly or identify a substitute plaintiff.

4. Dark-web trafficking should not lead the theory. The complaint alleges that stolen information is now likely available on the Dark Web. Caesars' May 19 notice says the opposite as of that date.[9]

[9] My investigation has not uncovered a verifiable 2026 dump.

5. NRS 603A-based negligence per se and NCFA predicates are mismatched to a Texas named plaintiff on a contact-and-DOB complaint, and the NCFA count cites outdated NRS 598.0923 subsection numbers. Correct the citations; prune 603A as to Huddleston; add a Nevada class representative if facts support.

6. The Privacy Policy disclaimer and Caesars' "no indication" notice language will be used against any implied-contract, unjust-enrichment, and risk theories. Plead specific cloud-platform and post-2023 remediation failures rather than breach-equals-negligence. SEC silence on a 2026 Form 8-K is useful contrast to the 2023 disclosure, not an independent liability element.

7. Judge Traum's related-case denial is not precedent. It remains useful architecture only if the 2026 pleading is repaired to high-sensitivity facts and plaintiff-specific injury consistent with *Zappos*, *Krottner*, and *Abdulaziz*.

IV. RELEVANT FACTUAL BACKGROUND

A. Operative pleading

The complaint alleges a second Caesars data breach in early 2026 after a September 2023 incident; that "Private Information" was accessible and unencrypted; and that exfiltrated information included, at a minimum, contact information and dates of birth. The class is defined as persons whose Private Information was compromised in the breach "discovered in March, 2026." Footnote 10 cites Melanie Porter, Gambling News (March 5, 2026), *Social Media Rumors: New Cyber Attack at Caesars?* Formal counts are negligence (with nested negligence per se), implied contract, unjust enrichment, and the Nevada Consumer Fraud Act. When the amended complaint was filed the same day as ECF 001, it deleted speculative Social Security number and driver's license allegations from the original complaint.

B. Official 2026 incident narrative

Caesars' May 19, 2026 consumer notice states that on February 23, 2026, Caesars identified suspicious activity in certain cloud-hosted platforms used to store data; activated incident-response protocols; engaged a cybersecurity firm; notified law enforcement; and reviewed affected data. Individual data fields are mail-merge placeholders in the public sample. Caesars states it has no indication that data has been published on the dark web or used for unauthorized transactions or identity theft, and offers two years of IDX identity-protection services. The Washington AG directory entry for May 19, 2026 lists 44,023 Washingtonians and information categories Name; Social Security Number; Driver's License or Washington ID Card Number; Full Date of Birth; Passport Number. Treat directory categories as official reporting metadata. They do not, standing alone, prove Huddleston's individual letter under *Greenstein*'s plaintiff-specific theft requirement.

C. SEC and corporate-control context

The September 14, 2023 Form 8-K, which belongs to the related case, admits a social-engineering attack on an outsourced IT support vendor and acquisition of loyalty-program database data including driver's license numbers and/or Social Security numbers. No analogous 2026 cybersecurity Form 8-K was located on Caesars' EDGAR 8-K index as of August 12, 2026. The March 31, 2026 Form 10-Q (filed April 28, 2026), refers to the 2023 "Data Incident" and generic future cybersecurity risk without disclosing a discrete 2026 consumer-data incident. Caesars' CSR Position on Data Privacy & Security (last updated September 2022) advertises a NIST-based program, incident-response planning, MFA, encryption, and a goal of managing guest and employee personal information "to ensure there can be no unauthorized use of or access to personal information."[10]

D. Related 2023 action

Mark Huddleston is a named Texas plaintiff and proposed Texas subclass representative in the consolidated 2023 Rewards breach litigation. On August 15, 2025, Judge Traum denied Caesars' motion to dismiss in full at the pleading stage, including Article III standing, on a complaint alleging highly sensitive data and misuse.

E. Open facts

No public source reviewed establishes that Huddleston personally received a May 2026 notice or that his data was in the 2026 affected population. Public open-web review has not established a verifiable 2026 dark-web sale or dump. Absolute nationwide headcount remains unresolved. The Washington litigation claimed 44,023 residents were affected, while secondary reports suggest "862" affected individuals.

V. ADVERSARIAL VULNERABILITIES AND OVERLOOKED FACTS

A. Standing on a self-limited pleading

Caesars will attack the complaint as pleading only contact information and date of birth, citing a rumor article, and failing to show that Huddleston's 2026 data was actually taken or that he was harmed. Under *TransUnion*, *Kisil*, and *Greenstein*, that is a weak damages-standing record. Caesars will also contend that mitigation or privacy injuries alone cannot reliably defeat that attack. Plaintiff's answer is factual repair of the 2026 record—the notice letter, official category evidence, and 2026-specific mitigation or misuse—not importation of 2023 injury chronology from the related case, and not Traum as controlling law in this action.

B. Wrong chronology, rumor sourcing, and dark-web rhetoric

Caesars will attack the class definition because it is keyed to a March 2026 "discovery" and rests on a Gambling News article titled as social-media rumor. The official record is different: Caesars identified suspicious activity on February 23, 2026, and mailed consumer notices dated May 19, 2026. Plaintiff's repair is to redefine the class around that official incident and to replace Gambling News as the primary source. Separately, drop dark-web trafficking as a lead allegation until commercial threat intelligence or discovery actually supports it. Caesars' May 19 notice says the opposite, and the public record does not yet show a verifiable 2026 dump.

C. Traceability and wrong-plaintiff risk

If Huddleston is not in the 2026 notice set, amendment cannot manufacture standing for him. Seek a substitute plaintiff or an extension rather than opposing on a wrong-plaintiff theory.

D. Nevada statutory theories for a Texas plaintiff

The stronger resolution is that NRS 603A-based negligence per se and NCFA predicates are mismatched to Huddleston on the current record. Correct NRS 598.0923 citations; prune 603A as to this plaintiff; add a Nevada class representative if facts support; evaluate Texas home-state claims only after 2026 injury facts and any pre-suit notice requirements are analyzed separately from the related case.

[10] Caesars Ent., Inc., *Position on Data Privacy & Sec. 3* (Sept. 2022), https://www.caesars.com/content/dam/empire/csr/policies-and-positions/pdf/csr-position-on-data-privacy-and-security.pdf.

E. Facts the complaint does not use

The complaint does not plead the cloud-hosted-platform vector now admitted in Caesars' own notice letters, the May 19, 2026 notice campaign, the IDX offer, or the Washington AG directory categories. It does not confront the "no indication of misuse" statement. It does not plead the contrast between the detailed September 2023 Form 8-K and the absence of a 2026 cybersecurity 8-K. It cites outdated NRS 598.0923 subsection numbers for the NCFA predicates. Namespace DNS recon shows Okta-, auth-, login-, VPN-, and marketing-cloud-named hosts in the caesars.com namespace; those are discovery leads, not proof of the breached platforms.

VI. DEFENSE FORECAST AND DISCOVERY PRIORITIES

A. Motion forecast

The motion to dismiss requests dismissal with prejudice and oral argument. Expect Caesars to (a) confine the Court to the complaint's contact-and-DOB allegations; (b) cite *TransUnion* together with *Kisil*- and *Greenstein*-style reasoning on low-sensitivity data, "may have been accessed" notice language, and the absence of misuse; (c) invoke *Popa* against bare privacy or statutory injuries; (d) distinguish Traum's order as a high-sensitivity, misuse-alleging pleading in a different case; (e) emphasize the Privacy Policy disclaimer and the May 19 "no indication" language once plaintiff cites the notices; (f) press economic-loss and *Sonner*-style arguments against negligence and unjust enrichment; and (g) attack Nevada statutory claims, including the mismatched NRS 598.0923 subsection citations, as to a Texas plaintiff. If plaintiff amends correctly, expect a renewed motion focused on plaintiff-specific injury, notice wording, and traceability rather than rumor sourcing.

B. Pre-opposition preservation and intake

Before opposition, counsel should lock down Huddleston's 2026 facts and the official notice record. Get a client declaration covering whether he received the May 2026 Caesars notice, any enrollment code, the exact wording ("may have been accessed" versus confirmed compromise), which data elements the notice listed, what time and money he spent on mitigation, and any 2026 misuse that is distinct from injuries alleged in the 2023 related case. If misuse is alleged, the declaration should set out a clean causation chronology.

Preserve the Massachusetts and Washington Attorney General notice materials, directory captures, and the May 19 consumer-notice template, with source and retrieval information.

Send a litigation hold covering Rewards profile data, 2026 notice lists, cloud-platform logs, incident-response materials, IDX and dark-web monitoring reports, and vendor contracts for the 2026 incident.

C. Posture-dependent discovery after pleading repair

These requests matter after the complaint is repaired. They are not a substitute for fixing standing first.

Ask Caesars to identify, for the February 2026 incident, exactly which data elements were involved and who was in the affected population. Ask which cloud-hosted platforms were involved, what access controls and MFA or other authentication were in place, and what the forensic reports show. Ask for the notice timeline: when Caesars detected the activity, how it scoped the incident, when it notified regulators, and when it notified consumers.

Discovery may also ask how the 2026 cloud platforms relate to what Caesars learned from the 2023 vendor social-engineering attack, including whether the later incident was foreseeable. That is a foreseeability question only. It does not treat the 2023 and 2026 incidents as the same breach.

VII. RECOMMENDATIONS TO STRENGTHEN PLAINTIFF'S POSITION

A. Immediate sequence (before September 4, 2026)

1. Complete Huddleston intake before August 20, 2026. Confirm whether he received a May 2026 Caesars or IDX letter; capture the letter and its exact compromise language.
2. By August 27, 2026, circulate a proposed amended complaint outline keyed to AG notices, plaintiff-specific facts, corrected NRS 598.0923(1)(b) and (1)(c) citations, and pruned 603A predicates. Archive current privacy policy, terms of service, Rewards rules, and CSR reports from caesars.com.
3. Prepare a Rule 15 amended complaint that (a) incorporates official February 23 and May 19 chronology and the cloud-platform vector; (b) pleads Washington directory categories as official incident-category reporting and Huddleston's letter fields as plaintiff-specific fact; (c) alleges concrete 2026 injury or mitigation without leading on unsupported dark-web trafficking; (d) corrects NRS 598.0923; and (e) prunes NRS 603A as a predicate for Huddleston individually unless a Nevada named plaintiff is added.
4. If amendment cannot be filed before September 4, seek leave concurrent with opposition and ask the Court to treat the motion as against the forthcoming pleading or to defer merits adjudication. If intake shows Huddleston is not in the 2026 set, identify a substitute plaintiff or seek extension; do not oppose on continuity alone.
5. Monitor for the consolidation motion referenced in ECF 8. Do not purchase purported stolen datasets from illicit markets; prefer preservation, commercial threat intelligence, and discovery into Caesars' and IDX dark-web monitoring consistent with Department of Justice Cybersecurity Unit guidance on lawful intelligence gathering.
6. Before any filed brief that treats case holdings as settled law, complete live citator and official-statute validation, including publication-status discipline for unpublished Ninth Circuit memoranda.

VIII. CONCLUSION

Both sides of the core disputes were tested. The weaker path is to oppose on ECF 004's contact-and-DOB, rumor-sourced pleading and hope Traum or generic mitigation theories carry the day. The stronger path is to treat the May 2026 official notices as the pleading backbone, insist on Huddleston-specific inclusion and data elements, correct the Nevada statutory citations, and only then meet Caesars' standing motion. This case has a real public-record backbone that the operative complaint does not use. The pending motion is designed to end the case on the complaint plaintiff chose to file on April 22—before consumer notices—and then narrowed on the same day by deleting the sensitive-data allegation. Done correctly, the motion becomes a standing fight on official notices and plaintiff-specific injury under the *Zappos* and *Krottner* line. Done incorrectly, it becomes a with-prejudice dismissal on a *Kisil*-style low-sensitivity record.