Michael J. Gayan
CLAGGETT & SYKES LAW FIRM
1160 N. Town Center Drive, Suite 200
Las Vegas, Nevada 89144
P: (702) 655-2346
mike@claggettlaw.com

John A. Yanchnis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor Tampa, Florida 33602
P: (813) 223-5505
jyanchunis@ForThePeople.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW8th Floor
Washington, D.C. 20005
P: (202) 408-4600
dmcnamara@cohenmilstein.com

Amy E. Keller
DICELLO LEVITT LLP
10 North Dearborn Street Sixth Floor
Chicago, Illinois 60602
P.: (312) 214-7900
akeller@dicellolevitt.com

Attorneys for Plaintiff and the Class

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 **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Mark Huddleston, individually and on behalf of the Class defined below of similarly situated persons ("Plaintiff and Class Members"), alleges the following against Defendant Caesars Entertainment, Inc. ("Caesars"). The following allegations are based on Plaintiff's knowledge, investigations by Plaintiff's counsel, facts of public record, and information and belief:

INTRODUCTION

1. Plaintiff seeks to hold Caesars responsible for the injuries it inflicted upon Plaintiff and others due to Caesars's inadequate data security, which resulted in the private information of Plaintiff and those similarly situated to be exposed to unauthorized third

parties (the "Data Breach").

2. Caesars is a publicly traded company incorporated in Delaware with its principal place of business at 100 West Liberty Street, 12th Floor, Reno, NV 89501. It is a global hospitality and gaming company that owns, operates, and manages hotels, casinos, and resorts located predominantly in Nevada. Caesars' portfolio of Las Vegas properties includes Caesars' Place Las Vegas, The Cromwell, Flamingo Las Vegas, Horseshoe Las Vegas, The LINQ Hotel & Casino, Paris Las Vegas, Planet Hollywood Resort & Casino, Harrah's Las Vegas, and Rio All-Suite and Casino.

3. In September, 2023, Caesars suffered a data breach, which exposed to the personal identifying information ("PII" or "Private Information") belonging to its clients – including the Plaintiff.

4. Despite having suffered a data breach as recently as 2023, Caesars failed to implement the requisite security measures, and failed to prevent another Data Breach from occurring in early 2026. Once again, Private Information belonging to Plaintiff and Class Members was taken by cybercriminals, exposing Class Members to an elevated and significant risk of fraud and identity theft.

5. Plaintiff and Class Members provided their Private Information to Caesars with the understanding and expressed or at least implied agreement that Caesars would keep that information private in accordance with both state and federal laws.

6. Caesars disregarded the rights of Plaintiff and Class Members by negligently failing to implement reasonable measures to safeguard Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. Caesars's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

7. Today, the Private Information of Plaintiff and Class Members continue to be in jeopardy because of Caesars's actions and inactions described herein. Plaintiff and Class Members now suffer from a present and continuing risk of fraud and identity theft for years to come and now must constantly monitor their financial and other accounts for

unauthorized activity.

8. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) anxiety, annoyance, and nuisance; (k) continued risk to their Private Information, which remains in Caesars's possession and is subject to further breaches so long as Caesars fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information; and (l) disgorgement damages associated with Caesars's maintenance and use of Plaintiff's data for its benefit and profit.

9. Through this action, Plaintiff seeks to remedy these injuries on behalf of himself and all similarly situated individuals whose Private Information was exposed and compromised in the Data Breach.

10. Plaintiff brings this action against Caesars and asserts claims for negligence, negligence *per se*, implied contract, unjust enrichment, and a violation of the Nevada Consumer Fraud Act.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over the action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs, there are more than 100 Class Members, and Plaintiff and at least one Class member is a citizen of a state different than Caesars.

12. This Court has general personal jurisdiction over Caesars because Caesars's

principal place of business is in this District. This Court also has specific personal jurisdiction over Caesars because Caesars engaged in the conduct underlying this action int his District, including the collection, storage, and inadequate safeguarding of Plaintiff's PII.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Caesars is based in this District, entered into consumer transactions with Plaintiff in this District, and made its data security decisions leading to the Data Breach in this District.

PARTIES

14. Plaintiff Mark Huddleston is a natural person, resident, and citizen of Texas. Plaintiff Huddleston has been a Caesars Reward member since 2007. Plaintiff Huddleston regularly gambled with Caesars both online and in person at which time Caesars regularly collected his PII.

15. Caesars, formally known as Eldorado Resorts, operates more than 50 casino gaming and resort properties throughout the United States. Caesars's customers come from a diverse, omni-channel base, primarily in the U.S., consisting of regional "drive-to" gamblers, high-value destination tourists in Las Vegas/Atlantic City, and younger digital sports bettors. Nearly 80% of the U.S. population is within a four-hour drive of a Caesars property, providing a stable local customer base.

FACTUAL ALLEGATIONS

A. Caesars Collects and Stores the Private Information of Plaintiff and Class Members

16. Plaintiff and Class Members provided their Private Information to Caesars as a requirement to obtain services from Caesars.

17. Caesars collects Private Information from Plaintiff and Class Members in the ordinary course of business. Upon information and belief, this Private Information is then stored on Caesars's systems.

18. Caesars knows that by collecting Private Information, it must comply with industry standards related to data security and all federal and state laws protecting Private

Information.

B. Caesars Uses Consumers' PII for Profit-Generating Purposes

19. Plaintiff and Class Members provided their Private Information to Caesars as a condition of receiving services from Caesars, but in doing so, expected Caesars to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

20. Caesars made promises and representations to its customers, including Plaintiff and Class Members, that the PII collected from them would be kept safe, confidential, that the privacy of that information would be maintained, and that Caesars would delete any sensitive information after it was no longer required to maintain it.

21. Caesars' current Privacy Policy states: "We maintain physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control. […]."[1]

22. Plaintiff and Class Members provided their PII to Caesars with the reasonable expectation and on the mutual understanding that Caesars would comply with its obligations to keep such information confidential and secure from unauthorized access.

23. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Caesars to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

24. Caesars had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Caesars has a legal duty to keep consumer's PII safe and confidential.

---

[1] https://www.caesars.com/corporate/privacy

25. Caesars had obligations created by the Federal Trade Commission Act ("FTC Act"), state law, contract, industry standards, and representations made to Plaintiff and Class Members to keep their PII confidential and to protect it from unauthorized access and disclosure.

26. Caesars derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Caesars could not perform the services it provides. Plaintiff's and Class Members' PII has an independent value to Caesars.

27. Caesars acknowledges in its privacy policy that it uses consumers' PII for the following purposes (among others):

- to operate our Caesars Rewards program and provide information to you about your Caesars Rewards program activity;
- to improve the products and services we provide you and develop new products and services;
- to improve our properties, websites and mobile apps;
- to track your use of our properties, websites and mobile apps for our internal market research and analytics;
- to create a more accurate and complete customer profile for you to better understand and predict the products and services you want to use and to provide a more personalized level of service;
- to notify you about promotions and special offers regarding products and services provided by us or our affiliates or other associated third parties, including our business partners;
- to ask for your participation in our internal market research;
- to generate aggregate statistical studies about our customers to better understand how our customers use our services; […][2]

28. Because of its use of Plaintiff's and Class Members' PII, Caesars sold more services and products than it otherwise would have.

29. Caesars was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create using Plaintiff's and Class Members' PII to the detriment of Plaintiff and Class Members.

30. Caesars' self-serving motive to retain and mine its customers' PII for its own financial benefit led to Caesars holding a trove of customer data. Caesars was unjustly

[2] *Id.*

enriched by retaining consumers' PII for its own profit motive, while failing to adopt reasonable data security measures to protect that PII.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Caesars assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

C. Caesars' Privacy Policy Represents That It Will Adequately Protect PII

32. Caesars' Privacy Policy touts its data security safeguards. The Privacy Policy makes materially false and misleading representations and omissions to Class Members. It states, in relevant part:

> Caesars Entertainment, Inc. and its subsidiaries and affiliates (referred to in this Privacy Policy as "Caesars," "us," "we," and/or "our") value you as a customer and are committed to respecting your data privacy. In the course of providing you with products and services, we may collect certain information from or about you. We are providing this Privacy Policy to explain our practices and policies for collecting, using and sharing information collected from or about you when you visit, access, or use, or provide information to us in connection with, one of our properties, websites or mobile Apps (referred to together as the "Caesars Services"). By visiting, accessing, or using, or providing information to us in connection with, the Caesars Services, you expressly consent to our collection, storage, use and sharing of your information as described in this Privacy Policy. Please note that if you disagree with anything in this Privacy Policy, you should not visit, access, or use, or provide information to us in connection with, the Caesars Services.
>
> […]
>
> **INFORMATION WE MAY COLLECT.**
> We collect and use information we believe is necessary to administer and promote our business, provide you with the products and services you request, and to provide a safe and healthy environment to our employees and other customers. We may collect and maintain both personal information and non-personal information needed for these purposes. Your personal information and/or non-personal information will be referred as your "information" in this Privacy Policy.
>
> […]
>
> **HOW WE COLLECT YOUR INFORMATION.**
> Information You Directly Provide to Us. You may provide information directly to us under a wide range of circumstances, such as when you submit information to us through our websites or mobile apps, use any gaming or non-gaming services at one of our properties, sign up to receive email or text messages from us, sign up to access Wi-Fi at a property, park at a property, install or use one of our mobile apps, sign up for Caesars Rewards, log in as a

> Caesars Rewards member, book a reservation for a property, enter an online promotion, request information from us, scan your ID at check-in kiosk at a property, apply for casino credit or provide feedback in a survey.
>
> […]
>
> **SECURITY.**
> We maintain physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control. With regard to information that you transfer to us through one of our websites or mobile apps, please be aware that no data transmission over the Internet or a wireless network can be guaranteed to be 100% secure. As a result, Caesars cannot guarantee or warrant the security of any information you transmit on or through a website or mobile app, and you do so at your own risk.[3]

33. These representations were misleading because, among other things, Caesars did not "maintain physical, electronic and organizational safeguards that reasonably and appropriately protect against the loss, misuse and alteration of the information under our control."[4]

34. The Privacy Policy also contained material omissions because it failed to disclose that Caesars' data security practices had significant shortfalls regarding its data systems that held consumers' PII.

35. Plaintiff and Class Members provided their PII to Caesars with the reasonable expectation and mutual understanding that Caesars would take reasonable steps to secure the PII from theft. Caesars failed to do so, in violation of its Privacy Policy and other legal duties discussed below.

D. Caesars Knew or Should Have Known it Faced a Serious Threat from and was a Likely Target of Cyber Criminals

36. The type of PII collected by the hospitality and accommodation industry makes it particularly appealing to cyber criminals.

37. Trustwave's "2018 Global Security Report" listed hospitality as one of the

[3] *Id.*
[4] *Id.*

top three industries most vulnerable to payment card breaches.[5] The report noted that there were 338 breaches in the accommodation industry in 2017 alone, including at many of the major hotel brands.

38. In recent years, Choice Hotels, Hard Rock Hotel, Hilton, Hyatt, Kimpton, Marriott, Millennium, Omni, Radisson, Starwood, and Wyndham, among others, have all experienced data breach incidents.[6] "Such unfortunate trends should not come as much of a surprise since hotels are hotbeds of sensitive information. Their data is spread out across porous digital systems…."[7]

39. While hospitality companies have fewer transactions than retail organizations— and thus have data on fewer customers to steal—they collect substantially more valuable and varied personal data for each of their guests. This rich personal data is invaluable to cybercriminals. They can use this data to better impersonate each breached customer, leading to additional identity theft and social engineering attacks. By enabling further attacks, breaching a hotel provides cybercriminals much more value than breaching a company in almost any other industry.[8]

40. The high risk of data breaches in the hotel industry was widely known throughout the field, including to Caesars.

41. In September 2023, Caesars suffered a major data breach after a social engineering attack on an IT vendor compromised the personal data of tens of millions of

---

[5] See Lena Combs & Joshua Davis, *Why Cybersecurity Matters*, Hotel Management (Oct. 17, 2019, 10:40 AM), https://www.hotelmanagement.net/tech/why-cybersecurity-matters.
[6] See *Timeline: The Growing Number of Hotel Data Breaches*, CoStar.com (April 7, 2020, 10:50 AM), available at https://www.costar.com/article/139958097 (last visited Sept. 27, 2023).
[7] *See* Combs, *supra*.
[8] Nirmal Kumar, *Cybersecurity in Hospitality: An Unsolvable Problem?*, HospitalityBiz (June 27, 2018) (now removed), https://web.archive.org/web/20211017182154/http:/www.hospitalitybizindia.com/detailNews.aspx?aid=28970&sid=42; The challenges of hospitality cybersecurity: An unsolved problem?, Deccan Chronicle (Aug. 23, 2018), https://www.deccanchronicle.com/technology/in-other- news/230818/the-challenges-of-hospitality-cybersecurity-an-unsolved-problem.html; *Cybersecurity in hospitality—a growing issue?*, CyberSmart (Mar. 23, 2021), https://cybersmart.com/2021/03/cybersecurity-in-hospitality-a-growing-issue/.

Caesars Rewards members.[9]

42. Thus, Caesars was clearly aware of the high risk of data intrusions and the magnitude of the harm that could result from a breach. Despite the known risks, Caesars failed to adopt reasonable safeguards to protect Class Members' PII after the 2023 data breach.

E. The Data Breach

43. Upon information and belief, Plaintiff's and Class Members' affected Private Information at the time of the Data Breach was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.[10]

44. Upon information and belief, Caesars was a target due to its status as an entity that collects, creates, and maintains Private Information.

45. Upon information and belief, the Private Information exfiltrated in the 2026 Data Breach included, at a minimum, Plaintiff's and Class Members' contact information and dates of birth.

46. Time is of the essence when highly sensitive Private Information is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired Private Information of Plaintiff and Class Members is now likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted Private Information to criminals.

47. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their Private Information. Plaintiff and Class Members face a lifetime risk of identity theft.

48. Caesars largely put the burden on Plaintiff and Class Members to take

---

[9] Caesars Form 8-K dated September 7, 2023: https://investor.caesars.com/static-files/0bc13ee5-34a9-402e-8e7a-824b9dba4e57.

[10] See Melanie Porter, "Social Media Rumors: New Cyber Attack at Caesars?", *Gambling News* (Mar. 5, 2026), https://www.gamblingnews.com/news/social-media-rumors-new-cyber-attack-at-caesars/, last accessed April 18, 2026.

measures to protect themselves from identity theft and fraud.

49. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members identity theft protection services for their respective lifetimes.

50. Plaintiff and the Class Members remain in the dark regarding exactly what data was stolen, the particular method of disclosure, the results of any investigations, and what steps are being taken, if any, to secure their Private Information going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly Caesars intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

51. Caesars could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers and systems, generally, as well as Plaintiff's and Class Members' Private Information.

52. Caesars's negligence in safeguarding Plaintiff's and Class Members' PII was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years and the 2023 Caesars data breach.

53. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.6% of U.S.-based workers are compensated on an hourly basis, while the other 44.4% are salaried.[11]

54. According to the American Time Use Survey, American adults have between 4 to 6 hours of "leisure time" outside of work per day;[12] examples of leisure time include partaking in sports, exercise and recreation; socializing and communicating; watching TV; reading; thinking/relaxing; playing games and computer use for leisure; and

---

[11] *Characteristics of minimum wage workers, 2022*, U.S. Bureau of Labor Statistics (Aug. 2023), https://www.bls.gov/opub/reports/minimum-wage/2022/home.htm (last accessed on Aug. 6, 2024).

[12] *Americans have no idea how to use their free time*, Business Insider (Mar. 26, 2024), https://www.businessinsider.com/americans-free-time-leisure-dont-use-television-2024-3 (last accessed on Aug. 6, 2024).

other leisure activities.[13] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

55. Plaintiff and Class Members are deprived of the choice as to how to spend their valuable free hours and therefore seek renumeration for the loss of valuable time as another element of damages.

F. The Value of PII

56. In April 2020, ZDNet reported in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for complaints as revenge against those who refuse to pay."[14]

57. In October 2023, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "malicious actors have adjusted their ransomware tactics to be more destructive and impactful and have also exfiltrated victim data and pressured victims to pay by threatening to release the stolen data."[15]

58. Stolen PII is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

---

[13] *Table 11A. Time spent in leisure and sports activities for the civilian population by selected characteristics, averages per day, 2022 annual averages*, U.S. Bureau of Labor Statistics (June 22, 2023), https://www.bls.gov/news.release/atus.t11A.htm (last accessed on Aug. 6, 2024).

[14] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNet (Apr. 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Jan. 17, 2024).

[15] *See StopRansomware Guide*, U.S. Cybersec. and Infrastructure Sec. Agency (Oct. 2023), https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf.

59. Malicious actors can use stolen personal information to, *inter alia*, create synthetic identities (which are harder for authorities to detect), execute credible phishing attacks, and sell the personal information on underground markets in the dark web.[16]

60. Another example is when the U.S. Department of Justice announced its seizure of RaidForums in 2022. RaidForums was an online marketplace popular for cybercriminals to purchase and sell hacked data belonging to millions of individuals around the world.[17] "One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[18]

61. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. According to Prey, a company that develops device tracking and recovery software, stolen PII and can be worth up to $2,000.00 depending on the type of information obtained.[19]

62. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

63. According to the FBI's Internet Crime Complaint Center (IC3) 2023 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and

---

[16] *What Data Do Cybercriminals Steal? (How To Protect Yours)*, Identity Guard (Feb. 14, 2024), https://www.identityguard.com/news/what-information-do-cyber-criminals-steal.
[17] *United States Leads Seizure of One of the World's Largest Hacker Forums and Arrests Administrator*, U.S. Dept. of Justice (Apr. 12, 2022), https://www.justice.gov/opa/pr/united-states-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator.
[18] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor (Apr. 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/.
[19] Juan Hernandez, *The Lifecycle of Stolen Credentials on the Dark Web*, Prey (Feb. 26, 2024), https://preyproject.com/blog/lifecycle-stolen-credentials-dark-web.

dollar losses that year, resulting in more than $12.5 billion in losses to individuals and business victims.[20]

64. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

65. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

66. For example, the United States Government Accountability Office ("GAO") noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[21] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[22]

67. The exposure of Plaintiff's and Class Members' PII to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

G. Caesars Failed to Comply with the Federal Trade Commission Act and Failed to Observe Reasonable and Adequate Date Security Measures

68. The Federal Trade Commission ("FTC") has issued several guides for

---

[20] *2023 Internet Crime Report*, Fed. Bureau of Investig. (2023), https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (last accessed Apr. 11, 2024).

[21] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao- 07-737.pdf (last visited Jan. 17, 2024).

[22] *Id*.

businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[23]

69. Under the FTC's 2016 *Protecting Personal Information: Guide for Business* publication, the FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[24]

70. The guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

71. The FTC advises companies not to keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[25]

72. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

73. Caesars's failure to employ reasonable and appropriate measures to protect

---

[23] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.

[24] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 17, 2024).

[25] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf.

against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

74. Plaintiff and Class Members gave their PII to Caesars with the reasonable expectation and understanding that Caesars would comply with its duty to keep such information confidential and secure from unauthorized access.

75. Caesars has been on notice for years that Plaintiff's and Class Members' PII was a target for bad actors because of, among other motives, the high value of the PII created, collected, and maintained by Caesars.

76. Despite such awareness, Caesars failed to impose and maintain reasonable and appropriate data security controls to protect Plaintiff's and Class Members' PII from unauthorized access that Caesars should have anticipated and guarded against.

77. Caesars was fully aware of its obligation to protect the PII of its customers because of its collection, storage, and maintenance of PII. Caesars was also aware of the significant consequences that would ensue if it failed to do so because Caesars collected, stored, and maintained sensitive private information from millions of individuals and knew that this information, if hacked, would result in injury to Plaintiff and Class Members.

78. Despite understanding the consequences of insufficient data security, Caesars failed to adequately protect Plaintiff's and Class Members' PII, permitting bad actors to access and misuse it.

H. Caesars Failed to Comply with Industry Standards

79. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes solutions to defend against those cyber-attacks.[26] All

[26] Center for Internet Security, *Critical Security Controls*, at 1 (May 2021), available at https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Jan. 17, 2024).

organizations collecting and handling PII, such as Caesars, are strongly encouraged to follow these controls.

80. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[27]

81. Several best practices have been identified that a minimum should be implemented by companies like Caesars, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[28]

82. Other best practices have been identified that a minimum should be implemented by companies like Caesars, including but not limited to ensuring that PII is only shared with third parties when reasonably necessary and that those vendors have appropriate cybersecurity systems and protocols in place.[29]

83. Caesars failed to follow these and other industry standards to adequately protect the PII of Plaintiff and Class Members.

I. The Data Breach Caused Harm and Will Result in Additional Fraud

84. Without detailed disclosure to the victims of the Data Breach, individuals whose PII was compromised by the Data Breach, including Plaintiff and Class Members, were unknowingly and unwittingly exposed to continued misuse and ongoing risk of misuse of their PII for months without being able to take available precautions to prevent imminent harm.

85. The ramifications of Caesars's failure to secure Plaintiff's and Class

---

[27] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Jan. 17, 2024).
[28] *See* Center for Internet Security, *Critical Security Controls* (May 2021), available at https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Jan. 17, 2024).
[29] *See id*.

Members' data are severe.

86. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.

87. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[30] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[31]

88. Identity thieves can use PII, such as that of Plaintiff and Class Members, which Caesars failed to keep secure, when combined with other information to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud, such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

89. As demonstrated herein, these and other instances of fraudulent misuse of the compromised PII has already occurred and are likely to continue.

90. Javelin Strategy and Research reports that identity thieves have stolen $43 billion in 2022.[32]

91. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. According to Experian, a credit monitoring company, "it takes an average of six months and roughly 200 hours of work to

---

[30] 17 C.F.R § 248.201 (2013).
[31] *Id.*
[32] *See Identity Fraud Losses Totaled $43 Billion in 2022, Affecting 40 Million U.S. Adults*, Javelin (Mar. 28, 2023), https://javelinstrategy.com/press-release/identity-fraud-losses-totaled-43-billion-2022-affecting-40-million-us-adults .

recover your identity after it's been compromised."[33]

92. There may be a time lag between when harm occurs versus when it is discovered, and also between when private information is stolen and when it is used. According to the U.S. GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[34]

93. Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

J. Plaintiff's Experience with the Data Breach

94. Plaintiff Huddleston provided his PII to Caesars—and upon information and belief, that PII was stored and maintained by Caesars.

95. Plaintiff values his privacy and makes every effort to keep his personal information private.

96. Plaintiff is now forced to live with the anxiety that his PII is being disclosed to the entire world, thereby subjecting Plaintiff to embarrassment and depriving him of any right to privacy whatsoever.

K. Plaintiff and Class Members Suffered Damages

97. The Data Breach was a direct and proximate result of Caesars's failure to properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Caesars's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII to protect against reasonably

---

[33] Gayle Soto, *The Unexpected Costs of Identity Theft*, Experian (Sept. 30, 2020), https://www.experian.com/blogs/ask-experian/what-are-unexpected-costs-of-identity-theft/

[34] GAO, *Report to Congressional Requesters*, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited Jan. 17, 2024).

foreseeable threats to the security or integrity of such information.

98. Had Caesars remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it would have prevented intrusion into its information storage and security systems and, ultimately, the theft of the PII of numerous individuals.

99. As a direct and proximate result of Caesars's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have already been harmed by the fraudulent misuse of their PII, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

100. Caesars's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their PII;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market; and,

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

101. While Plaintiff's and Class Members' PII has been stolen, Caesars continues to hold Plaintiff's and Class Members' PII. Particularly because Caesars has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

102. Plaintiff brings this class action individually and on behalf of all similarly situated persons under Federal Rule of Civil Procedure 23. Plaintiff seeks certification under Federal Rule of Civil Procedure 23(a), (b)(2), and (b)(3) of the following Nationwide Class (the "Class"):

> All persons in the United States whose Private Information was compromised in the Caesars's Data Breach discovered in March, 2026.

103. The Class defined above is readily ascertainable from information in Caesars's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

104. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Caesars, Caesars's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Caesars or their parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Caesars's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

105. Plaintiff reserves the right to amend or modify the Class definitions as this case progresses.

106. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

107. **Numerosity**. Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of thousands of individuals whose PII were compromised by Caesars's Data Breach.

108. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If Caesars unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. If Caesars failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. If Caesars's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. If Caesars's data security systems prior to and during the Data Breach were

consistent with industry standards;

e. If Caesars owed a duty to Class Members to safeguard their PII;

f. If Caesars breached its duty to Class Members to safeguard their PII;

g. If Caesars knew or should have known that its data security systems and monitoring processes were deficient;

h. If Caesars should have discovered the Data Breach earlier;

i. If Caesars took reasonable measures to determine the extent of the Data Breach after it was discovered;

j. If Caesars's delay in informing Plaintiff and Class Members of the Data Breach was unreasonable;

k. If Caesars's method of informing Plaintiff and Class Members of the Data Breach was unreasonable;

l. If Caesars's conduct was negligent;

m. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Breach;

n. If Plaintiff and Class Members suffered legally cognizable damages as a result of Caesars's misconduct;

o. If Caesars breached implied contracts with Plaintiff and Class Members;

p. If Caesars was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

q. If Caesars failed to provide notice of the Data Breach in a timely manner, and;

r. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

109. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach. Moreover, Plaintiff and Class Members were subjected to Caesars's uniformly illegal and impermissible conduct.

110. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's counsel is competent and experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

111. **Predominance**. Caesars has engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' data was stored on the same computer system and unlawfully exposed in the same way. The common issues arising from Caesars's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

112. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Caesars. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

113. The litigation of the claims brought herein is manageable. Caesars's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

114. Adequate notice can be given to Class Members directly using information maintained in Caesars's records.

115. Likewise, particular issues under Federal Rule of Civil Procedure 23(c)(4) are appropriate for certification because such claims present only particular, common

issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above.

116. Caesars has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CLAIMS FOR RELIEF

COUNT I: NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE CLASS)

117. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 116 of the Complaint as if fully set forth herein.

118. As a condition of receiving Caesars' services, Plaintiff and all Class Members were obligated to provide Caesars with their PII.

119. Plaintiff and Class Members entrusted their PII to Caesars with the understanding that Caesars would take reasonable measures to safeguard their PII.

120. Caesars had knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could face if their PII was stolen in a data breach.

121. Caesars had a duty to exercise reasonable care in safeguarding, securing, and protecting Class Members' PII. This duty included, among other things, designing, maintaining, and testing Caesars' data security procedures to ensure that the PII was adequately protected, that cloud-based safeguards were adequately implemented, and that employees tasked with maintaining PII were adequately trained on cyber security measures.

122. Caesars' duty of care arose from, among other things:

- the special relationship that existed between Caesars and its customers because, e.g., Caesars was in an exclusive position to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur;
- Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and

enforced by the FTC, failing to adopt reasonable data security measures;

- Caesars' representations in its Privacy Policy;
- General common law duties to adopt reasonable data security measures to protect customer PII and to act as a reasonable and prudent person under the same or similar circumstances would act; and
- State statutes requiring reasonable data security measures, including but not limited to Nev. Rev. Stat. § 603A.210, which states that businesses possessing personal information of Nevada residents "shall implement and maintain reasonable security measures to protect those records from authorized access."

123. Caesars was subject to an "independent duty," untethered to any express contract between Caesars and Class Members. Sources of the independent duty are included in the list above.

124. Caesars' violation of the FTC Act and state data security statutes constitutes negligence per se for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the type of harm that resulted from the Data Breach.

125. Plaintiff and Class Members were the foreseeable victims of Caesars' inadequate data security practices. Caesars knew that a breach of its systems could cause harm to Plaintiff and Class Members.

126. Caesars' conduct created a foreseeable risk of harm to Plaintiff and Class Members. Caesars' misconduct included its failure to adequately restrict access to its cloud server that held consumers' PII.

127. Caesars knew or should have known of the inherent risks in collecting and storing PII, the importance of providing adequate data security, and the frequent cyberattacks aimed at the hotel industry.

128. Plaintiff and Class Members had no ability to protect their PII once it was in Caesars' possession and control. Caesars was in an exclusive position to protect against the

harm suffered by Plaintiff and Class Members as a result of the Data Breach.

129. Caesars, through its actions and inactions, breached its duties owed to Plaintiff and Class Members by failing to exercise reasonable care in safeguarding their PII while it was in Caesars' possession and control.

130. Caesars inadequately safeguarded consumers' PII in deviation of standard industry rules, regulations, and best practices at the time of the Data Breach.

131. But for Caesars' breach of duties, consumers' PII would not have been stolen by a computer hacker.

132. There is a temporal and close causal connection between Caesars' failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiff and Class Members.

133. As a result of Caesars' negligence, Plaintiff and Class Members suffered and will continue to suffer the various types of damages alleged herein—including, but not limited to, significant risk of substantial and immediate future harm, identity theft and fraud, additional time, resources, and money spent on mitigation efforts, increased phishing and attempts at fraud, and further loss of value of personal information.

134. Due to Caesars's conduct, Plaintiff and Class Members are also entitled to identity protection and credit monitoring. Identity protection and credit monitoring is reasonable here. The PII taken can be used towards identity theft and other types of financial fraud against the Class Members. The consequences of identity theft are serious and longlasting. There is a benefit to early detection and monitoring. Some experts recommend that data breach victims obtain credit monitoring services for many years after a data breach.

135. Plaintiff and Class Members are entitled to all forms of monetary compensation and injunctive relief set forth above.

COUNT II: BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

136. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 116 of the Complaint as if fully set forth herein.

137. When Plaintiff and Class Members provided consideration and PII to Caesars in exchange for Caesars' services, they entered into implied contracts with Caesars under which Caesars agreed to adopt reasonable steps to protect their PII.

138. Caesars solicited and invited Plaintiff and Class Members to purchase its services. As part of that process, Plaintiff and Class Members were required to provide their PII.

139. When entering into the implied contracts, Plaintiff and Class Members reasonably believed and expected that Caesars would implement reasonable and adequate data security measures and that Caesars' data security practices complied with relevant laws, regulations, and industry standards. Caesars knew or reasonably should have known that Plaintiff and Class Members held this belief and expectation.

140. When entering into the implied contracts, Caesars impliedly promised to adopt reasonable data security measures. Caesars required consumers to provide their PII during the reservation and/or check-in process. In doing so, Caesars made implied or implicit promises that its data security practices were reasonably sufficient to protect consumers' PII. By virtue of accepting Plaintiff's PII during the reservation and check-in process, Caesars implicitly represented that its data security processes were reasonably sufficient to safeguard the PII.

141. Caesars' conduct in requiring consumers to provide PII as a prerequisite to the use of Caesars' services illustrates Caesars' intent to be bound by an implied promise to adopt reasonable data security measures.

142. Plaintiff and Class Members would not have provided their PII to Caesars in the absence of Caesars' implied promise to keep the PII reasonably secure.

143. Plaintiff and Class Members fully performed their obligations under the implied contracts with Caesars. They provided consideration and their PII to Caesars in exchange for Caesars' services and its implied promise to adopt reasonable data security

safeguards.

144. Caesars breached its implied contracts with Plaintiff and Class Members by failing to implement reasonable data security measures.

145. As a result of Caesars' conduct, Plaintiff and Class Members have suffered, and continue to suffer, legally cognizable damages arising from the Data Breach as set forth above.

146. Plaintiff and Class Members are entitled to all forms of monetary compensation and injunctive relief set forth herein.

COUNT III: UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE CLASS)

147. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 116 of the Complaint as if fully set forth herein.

148. This claim is pled in the alternative to the breach of implied contract claim.

149. Plaintiff and Class Members conferred monetary benefits on Caesars.

150. In exchange, Plaintiff and Class Members should have received Caesars' services as well as adequate safeguarding of their PII.

151. Caesars profited from its transactions with Class Members in two ways. First, Caesars received monetary consideration as revenue. Second, Caesars used Class Members' PII for a variety of profit-generating purposes beyond simply providing its services. Caesars used the PII for marketing and other purposes discussed more fully above. Caesars used the PII to generate future stays from consumers and derive future revenues and profit.

152. The money Plaintiff and Class Members paid to Caesars was intended to be used by Caesars, in part, to fund Caesars' costs of providing reasonable data security.

153. Caesars failed to provide reasonable data security, yet it kept all monies paid by Plaintiff and Class Members.

154. Caesars knew that Plaintiff and Class Members conferred monetary and other benefits on Caesars. Caesars accepted those benefits.

155. Under principles of equity and good conscience, Caesars should not be permitted to retain the full monetary benefit of its transactions with Plaintiff and Class Members. Caesars failed to adequately secure consumers' PII and, therefore, did not provide the full services that consumers paid for.

156. Caesars acquired consumers' money and PII through inequitable means in that it failed to disclose its inadequate data security practices when entering into transactions with consumers and obtaining their PII.

157. If Plaintiff and Class Members would have known that Caesars employed inadequate data security safeguards, they would not have agreed to provide Caesars with their PII or required Caesars to increase their security.

158. Class Members have no adequate remedy at law. Caesars continues to retain Class Members' PII while exposing the PII to a risk of future data breaches while in Caesars' possession. Caesars also continues to derive a financial benefit from using Class Members' PII.

159. As a direct and proximate result of Caesars' conduct, Plaintiff and Class Members have suffered the various types of damages alleged herein.

160. Caesars should be compelled to disgorge into a common fund or constructive trust, for the benefit of Class Members, the proceeds that they unjustly received from Class Members. In the alternative, Caesars should be compelled to refund the amounts that Class Members overpaid for Caesars' services.

COUNT IV: VIOLATION OF THE NEVADA CONSUMER FRAUD ACT NEV. REV. STAT. § 41.600 (ON BEHALF OF PLAINTIFF AND THE CLASS)

161. Plaintiff re-alleges and incorporates by reference paragraphs 1 to 116 of the Complaint as if fully set forth herein.

162. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600, states:

> 1. An action may be brought by any person who is a victim of consumer fraud.
> 2. As used in this section, "consumer fraud" means: . . . (e) A deceptive

trade practice as defined in NRS 598.0915 to 598.0925, inclusive.

163. In turn, Nev. Rev. Stat. § 598.0923(2) (a section of the Nevada Deceptive Trade Practices Act) states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . 2) Fails to disclose a material fact in connection with the sale or lease of goods or services." Caesars violated this provision because it failed 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. Caesars knew or should have known that its data security practices were deficient. This is true because, among other things, Caesars was aware that the hotel industry was a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its cloud server data security practices were insufficient to guard against those attacks. Caesars had knowledge of the facts that constituted the omission. Caesars could and should have made a proper disclosure when accepting hotel reservations, during the check-in process, in the registration for its Caesars Rewards loyalty program, in its Privacy Policy, or by any other means reasonably calculated to inform consumers of its inadequate data security.

164. Also, Nev. Rev. Stat. § 598.0923(3) states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . 3) Violates a state or federal statute or regulation relating to the sale or lease of . . . services." Caesars violated this provision for several reasons, each of which is an independent predicate act for purposes of violating § 598.0923(3).

165. *First*, Caesars breached a Nevada statute requiring reasonable data security. Specifically, Nev. Rev. Stat. § 603A.210(1) states: "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 from unauthorized access, acquisition, . . . use, modification or disclosure." (Emphasis added.) Caesars is a data collector as defined under the statute at Nev. Rev. Stat. § 603A.030. Caesars failed to implement and maintain reasonable security measures, evidenced by the fact that hackers

accessed its cloud server and stole consumers' PII. Caesars' violation of this statute was done knowingly for purposes of Nev. Rev. Stat. § 598.0923(3). Caesars knew or should have known that its data security practices were deficient. This is true because, among other things, Caesars was aware that the hotel industry was a frequent target of sophisticated cyberattacks. Caesars knew or should have known that its cloud server data security practices were insufficient to guard against those attacks. Caesars had knowledge of the facts that constituted the violation.

166. *Second*, Caesars breached other state statues as alleged herein. Caesars also violated Nev. Rev. Stat. § 598.0923(2) as alleged in this Count. Caesars knew or should have known that it violated these statutes. Caesars' violation of each of these statutes serves as a separate predicate act for purposes of violating Nev. Rev. Stat. § 598.0923(3).

167. *Third*, Caesars violated the FTC Act, 15 U.S.C. § 45, as alleged above. Caesars knew or should have known that its data security practices were deficient, violated the FTC Act, and that it failed to adhere to the FTC's data security guidance for businesses. This is true because, among other things, Caesars was aware that the hospitality and gaming industries were a frequent target of sophisticated cyberattacks, including the Caesars breach in 2023. Caesars knew or should have known that its cloud server data security practices were insufficient to guard against those attacks. Caesars had knowledge of the facts that constituted the violation. Caesars' violation of the FTC Act serves as a predicate act for violating Nev. Rev. Stat. § 598.0923(3).

168. Caesars engaged in deceptive or unfair practices by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Class Members.

169. Plaintiff and Class Members were denied a benefit conferred on them by the Nevada legislature.

170. Nev. Rev. Stat. § 41.600(3) states that if the plaintiff prevails, the court "shall award: (a) Any damages that the claimant has sustained; (b) Any equitable relief that the court deems appropriate; and (c) the claimant's costs in the action and reasonable attorney's fees."

171. As a direct and proximate result of the foregoing, Plaintiff and Class Members suffered all forms of damages alleged herein. Plaintiff's harms constitute compensable damages under Nev. Rev. Stat. § 41.600(3).

172. Plaintiff and Class Members are also entitled to all forms of injunctive relief sought herein.

173. Plaintiff and Class Members are also entitled to an award of their attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, on behalf of himself and all others similarly situated, request the following relief:

A. An Order certifying this case as a class action;

B. An Order appointing Plaintiff as a class representatives;

C. An Order appointing the undersigned counsel as class counsel;

D. Injunctive relief requiring Caesars to: (i) strengthen its data security systems and procedures; (ii) submit to future annual audits of those systems by a Court appointed independent auditor; and (iv) delete PII that Caesars no longer needs for processing services previously provided to Class Members;

E. An award of nominal damages, compensatory damages, money for significant and reasonable credit monitoring, statutory damages, treble damages, and punitive damages;

F. An award of Plaintiff's attorneys' fees and litigation costs; and

G. Such other and further relief as this Court may deem just and proper.

/ / /

/ / /

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Complaint so triable.

Dated this 22nd day of April, 2026.

Respectfully Submitted,

CLAGGETT & SYKES LAW FIRM

/s/ Michael Gayan

Michael J. Gayan (#11135)
1160 N. Town Center Drive, Suite 200
Las Vegas, Nevada 89144
mike@claggettlaw.com

Douglas J. McNamara*
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 8th Floor
Washington, D.C. 20005
dmcnamara@cohenmilstein.com

Amy E. Keller*
DICELLO LEVITT LLP
10 North Dearborn Street, Sixth Floor
Chicago, Illinois 60602
akeller@dicellolevitt.com

John A. Yanchunis*
MORGAN & MORGAN COMPLEX
LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
jyanchunis@forthepeople.com

Jeff Ostrow*
KOPRLOWITZ OSTROW, P.A.
1 West Las Olas Blvd, 5th Floor
Ft. Lauderdale, Florida 33301
ostrow@kolawyers.com

James Pizzirusso*
HAUSFELD LLP
888 16th Street N.W., Suite 300
Washington, D.C. 20006
jpizzirusso@hausfeld.com

Gerard Stranch*
STRANCH, JENNING & GARCEY, PLLC
223 Rosa L Parks Ave, Suite #200
Nashville, Tennessee 37203
gstranch@stranchlaw.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite #2100
Chicago, Illinois 60606
gklinger@milberg.com

Sabita J. Soneji*
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, California 94612
ssoneji@tzlegal.com

Linda P. Nussbaum*
NUSSBAUM LAW GROUP, P.C.
1133 Avenue of the Americas, 31st Floor
New York, New York 10036
lnussbaum@nussbaumpc.com

Counsel for Plainitff and the Proposed Class

**pro hac vice forthcoming*