

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

Master File No. 2:23-cv-01480

(Consolidated for pretrial proceedings with Case Nos. 2:23-cv-1481, 2:23-cv-1537, 2:23-cv-1549, 2:23-cv-1550, 2:23-cv-1577, 2:23-cv-1698, 2:23-cv-1719, 2:23-cv-1777, 2:23-cv-1826, 2:23-cv-1981, 2:23-cv-2042, 2:23-cv-2064, 2:24-cv-81)

In re: MGM Resorts International Data Breach Litigation

This document relates to: All actions.

CONSOLIDATED CLASS ACTION

Case No. 2:23-cv-01480

CONSOLIDATED CLASS ACTION COMPLAINT

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs, Tonya Owens, Emily Kirwan, David Zussman, David Lackey, Michael Pircio, David Terezo, Ronald G. Rundell, Anita Johnson, Paul Zari, Michael Manson, Kyle Sloan, Michelle Righetti, Edgar Mejia, and DuJun Johnson (“Plaintiffs”), individually, and on behalf of all others similarly situated (“Class Members”) allege the following against Defendant, MGM Resorts International (“MGM” or Defendant”) based on personal knowledge as to themselves and on information and belief as to the other allegations derived from, among other things, the investigation of the undersigned counsel:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to prevent a cyberattack that resulted in Plaintiffs’ and other similarly situated MGM consumers’—the Class Members’—sensitive information, including, upon information and belief, their full names, dates of birth, addresses, email addresses, phone numbers, Social Security numbers and/or driver’s

1 license numbers (“personally identifiable information” or “PII”).¹

2 2. Beginning on September 7, 2023, hackers gained access to Defendant’s network by
3 impersonating an IT admin and gaining access credentials. The hackers then locked down
4 Defendant’s network preventing resort guests from using their electronic room cards, Wi-Fi, ATM
5 kiosks, electronic gaming devices, and other resort services.

6
7 3. Two cybercriminal groups have taken credit for the attack against Defendant. First,
8 a hacking group known as "The Scatter Spider" took credit, on or about September 11, 2021, for
9 accessing and acquiring "six terabytes of data from the systems of multibillion-dollar casino
10 operators MGM Resorts International[.]”² Second, a ransomware group known as ALPHV took
11 credit, on or about September 14, 2023, for deploying a ransomware attack against Defendant and
12 "download[ing] any and all exfiltrated materials", including "PII information contained in the
13 exfiltrated data[]" involved in the cyberattack.³ Though both groups took credit, they are likely
14 operating as the same group, as are largely considered to be related.

15
16 4. Defendant owns and operates casino gaming brands with resorts throughout the
17 United States, which include dining, live entertainment, accommodations, shopping, and gaming.

18 5. Upon information and belief, individuals, including Plaintiffs and Class Members,
19 who were consumers of Defendant's entertainment services or sought to join the MGM Rewards
20

21
22
23 ¹ Bill Toulas, *MGM Resorts Ransomware Attack Led to \$100 Million Loss, Data Theft*, (Oct. 6,
24 2023), <https://www.bleepingcomputer.com/news/security/mgm-resorts-ransomware-attack-led-to-100-million-loss-data-theft>.

25 ² Zeba Siddiqui, *Hackers Say They Stole 6 Terabytes of Data from Casino Giants MGM, Caesars*
26 (Sept. 14, 2023), <https://www.reuters.com/business/casino-giant-caesars-confirms-data-breach-2023-09-14>.

27 ³ *Statement on MGM Resorts International: Setting the Record Straight* (Sept. 14, 2023),
28 <https://gist.githubusercontent.com/BushidoUK/20b81335c6729dc8e0b5997ca83fa35f/raw/a0697117e905f5094e7a5feae928806b2ba65b20/gistfile1.txt>.

1 loyalty program are required to entrust Defendant with sensitive, non-public PII, without which
2 Defendant could not perform its regular business activities, to obtain entertainment products and/or
3 services from Defendant. Defendant retains this information for at least many years and even after
4 the consumer relationship has ended.

5
6 6. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and
7 Class Members, Defendant assumed legal and equitable duties to those individuals to protect and
8 safeguard that information from unauthorized access and intrusion.

9 7. Defendant failed to adequately protect Plaintiffs’ and Class Members PII—and
10 failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII
11 was compromised due to Defendant’s negligent and/or careless acts and omissions and its utter
12 failure to protect consumers’ sensitive data. Hackers targeted and obtained Plaintiffs’ and Class
13 Members’ PII because of its value in exploiting and stealing the identities of Plaintiffs and Class
14 Members. The present and continuing risk to victims of the Data Breach will remain for their
15 respective lifetimes.
16

17 8. Defendant is a gaming and hospitality company that owns and operates 31 hotel
18 and gaming destinations globally, including 12 hotels on the Las Vegas Strip. MGM is a publicly
19 traded company and listed on the NASDAQ stock exchange with the ticket symbol “MGM”.⁴
20

21 9. Plaintiffs bring this action on behalf of all persons whose PII was compromised as
22 a result of Defendant’s failure to: (i) adequately protect the PII of Plaintiffs and Class Members;
23 (ii) warn Plaintiffs and Class Members of Defendant’s inadequate information security practices;
24

25
26 _____
27 ⁴ MGM Resorts International, Securities and Exchange Commission Form 8-k,
28 <https://www.sec.gov/ix?doc=/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm>.

1 and (iii) effectively secure hardware containing protected PII using reasonable and effective
2 security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to
3 negligence and violates federal and state statutes.

4 10. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally,
5 willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable
6 measures, failing to take available steps to prevent an unauthorized disclosure of data, and failing
7 to follow applicable, required, and appropriate protocols, policies, and procedures regarding the
8 encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was
9 compromised through disclosure to an unknown and unauthorized third party.
10

11 11. Plaintiffs and Class Members have a continuing interest in ensuring that their
12 information is and remains safe, and they should be entitled to injunctive and other equitable relief.
13

14 12. Plaintiffs and Class Members have suffered injury as a result of Defendant's
15 conduct. These injuries include: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished
16 value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual
17 consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs
18 associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the
19 continued and certainly increased risk to their PII, which: (a) remains unencrypted and available
20 for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's
21 possession and is subject to further unauthorized disclosures so long as Defendant fails to
22 undertake appropriate and adequate measures to protect the PII.
23

24 13. Plaintiffs seek to remedy these harms and prevent any future data compromise on
25 behalf of themselves and all similarly situated persons whose personal data was compromised and
26 stolen because of the Data Breach and who remain at risk due to Defendant's inadequate data
27
28

1 security practices.

2 **II. PARTIES**

3 14. Defendant is a Delaware corporation with its principal place of business in the State
4 of Nevada at 3600 South Las Vegas Boulevard, Las Vegas, Nevada 89109.

5 15. Plaintiff Tonya Owens is a natural person and is a resident and citizen of the State
6 of Mississippi, where she intends to remain.

7 16. Plaintiff Emily Kirwan is a natural person and is a resident and citizen of the State
8 of Louisiana, where she intends to remain.

9 17. Plaintiff David Zussman is a natural person and is a resident and citizen of the State
10 of Texas, where he intends to remain.

11 18. Plaintiff David Lackey is a natural person and is a resident and citizen of the
12 Commonwealth of Virginia, where he intends to remain.

13 19. Plaintiff Michael Pircio is a natural person and is a resident and citizen of the State
14 of Ohio, where he intends to remain.

15 20. Plaintiff David Terezo is a natural person and is a resident and citizen of the State
16 of New York, where he intends to remain.

17 21. Plaintiff Ronald G. Rundell is a natural person and is a resident and citizen of the
18 State of South Dakota, where he intends to remain.

19 22. Plaintiff Anita Johnson is a natural person and is a resident and citizen of the State
20 of California, where she intends to remain.

21 23. Plaintiff Paul Zari is a natural person and is a resident and citizen of the
22 Commonwealth of Virginia, where he intends to remain.

23 24. Plaintiff Michael Manson is a natural person and is a resident and citizen of the
24

1 State of Arizona, where he intends to remain.

2 25. Plaintiff Kyle Sloan is a natural person and is a resident and citizen of the State of
3 Indiana, where he intends to remain.

4 26. Plaintiff Michelle Righetti is a natural person and is a resident and citizen of the
5 State of California, where she intends to remain.

6 27. Plaintiff Edgar Mejia is a natural person and is a resident and citizen of the State of
7 Nevada, where he intends to remain.

8 28. Plaintiff DuJun Johnson is a natural person and is a resident and citizen of the State
9 of Nevada, where he intends to remain.

10
11 **III. JURISDICTION AND VENUE**

12 29. The Court has subject matter jurisdiction over this action under the Class Action
13 Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds five million dollars,
14 exclusive of interest and costs. Indeed, there are more than seventy-five million Class Members,
15 and numerous plaintiffs who reside in diverse states.

16 30. This Court has jurisdiction over Defendant because it operates in this District.

17 31. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because
18 Defendant's principal place of business is located in this District, a substantial part of the events
19 giving rise to this action occurred in this District, and Defendant has harmed Class Members
20 residing in this District.
21

22
23 **IV. GENERAL FACTUAL ALLEGATIONS**

24 ***The Data Breach***

25 32. On September 11, 2023, MGM posted a message on social media informing
26
27
28

1 consumers that MGM experienced a cybersecurity issue affecting some of its systems.⁵

2 33. Through its investigation, MGM determined that an unauthorized actor acquired,
3 among other data, names, contact information (such as phone numbers, email addresses, and postal
4 addresses), genders, dates of birth, and driver's license numbers of certain customers, and for some
5 customers, social security numbers and/or passport numbers.⁶

7 34. According to news reports, the unauthorized actor is a hacking group known as
8 Scattered Sider (or UNC3944) which is known for using social engineering to trick employees of
9 the target company into granting them access to their network.⁷

10 35. On or around October 5, 2023, MGM filed a Form 8-K with the SEC to alert
11 investors and shareholders that the Data Breach will have a negative impact on third quarter 2023
12 results.⁸

14 36. Also, around that time, MGM published an informational website regarding the
15 Data Breach. While the website did not provide much detail about the scope and breadth of the
16 Breach, it did state that at a minimum that phone numbers, email addresses, postal addresses,
17 genders, dates of birth, and driver's license numbers of some of its customers were impacted, and
18 that for a certain number of customers, social security numbers and/or passport numbers were also
19 affected.⁹ MGM stated that it is offering credit monitoring and identity theft protection services to
20

21
22 ⁵ See Sean Morrison, *The Chaotic and Cinematic MGM Casino Hack, Explained*, VOX,
23 <https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware>.

24 ⁶ Notice of Data Breach, <https://www.mgmresorts.com/en/notice-of-data-breach.html>.

25 ⁷ Carly Page & Zack Whittaker, *Hackers claim MGM cyberattack as outage drags into fourth day*,
26 TECHCRUNCH (Sept. 14, 2023), <https://techcrunch.com/2023/09/14/mgm-cyberattack-outage-scattered-spider>.

27 ⁸ SEC Form 8-K, *supra* n.4.

28 ⁹ Notice of Data Breach, *supra* n.6.

1 customers impacted by the Data Breach.¹⁰

2 37. Plaintiffs' investigation has revealed that, in early summer 2023, hackers began
3 intelligence gathering on MGM to identify employees and contractors that might have
4 administrator level privileges to the MGM information systems. The hackers then began contacting
5 the MGM help desk to impersonate those individuals and to convince the MGM help desk
6 employees to reset the target's password, so that the hackers would have access to that MGM
7 employee or contractor's account.
8

9 38. Ultimately, the hackers compromised multiple accounts, including administrator
10 credentials.

11 39. Though not definitive, Plaintiffs' investigation revealed that data taken from
12 MGM's systems has likely been circulated around the dark web.
13

14 40. Moreover, Plaintiffs' investigation revealed that the hackers likely exploited
15 Defendant's help desk by convincing members of the IT help desk to reset passwords, allowing
16 the hackers to gain initial access.

17 41. MGM is responsible for allowing the Data Breach to occur because it failed to
18 implement and maintain reasonable safeguards, failed to comply with industry-standard data
19 security practices, as well as federal and state laws and regulations governing data security, and
20 failed to supervise, monitor, and oversee all third parties it hired who had access to Plaintiffs' and
21 the Class Members' PII.
22

23 42. During the Data Breach, MGM failed to adequately monitor its information
24 technology infrastructure. Had MGM done so, it would have prevented or mitigated the scope and
25

26
27 ¹⁰ *Id.*
28

1 impact of the Data Breach.

2 43. Plaintiffs and Class Members provided their PII to MGM with the reasonable
3 expectation and mutual understanding that MGM would comply with its obligations to keep such
4 information confidential and secure from unauthorized access.

5 44. MGM's data security obligations were particularly important given the substantial
6 increase in cyber and ransomware attacks and data breaches in the gaming and hospitality
7 industries preceding the date of the Data Breach, as well as given the incredibly sensitive nature
8 of PII that it retained in its servers.

9 45. By obtaining, collecting, and using Plaintiffs' and Class Members' PII, MGM
10 assumed legal and equitable duties and knew or should have known that it was responsible for
11 protecting Plaintiffs' and Class Members' PII from disclosure.

12 46. As a result of MGM's failure to protect sensitive PII it was entrusted with, Plaintiffs
13 and Class Members are at a significant risk of identity theft, financial fraud, and other identity-
14 related fraud into the indefinite future. Plaintiffs and Class Members have also lost the inherent
15 value of their PII.

16 ***MGM Was on Notice of Data Breach Threats and the Inadequacy of Its Data Security***

17 47. MGM's data security obligations were especially important given the substantial
18 increase in cyberattacks and data breaches in recent years. In 2022, there were 1,802 reported data
19 breaches, affecting approximately 422 million individuals.¹¹

20 48. MGM should have been aware—and was aware—that it was at risk of an internal
21 data breach that could expose the PII that it collected and maintained.

22
23
24
25
26
27 ¹¹ 2022 Data Breach Report, IDENTITY THEFT RES. CTR., https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf, at 2.

1 49. Despite this, MGM failed to take the necessary precautions required to safeguard
2 Plaintiffs' and Class Members' PII from unauthorized access.

3 ***MGM Failed to Comply with Statutory and Regulatory Obligations***

4 50. Federal and State governments have established security standards and issued
5 recommendations to minimize data breaches and the resulting harm to individuals and financial
6 institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses
7 that highlight the importance of reasonable data security practices. According to the FTC, the need
8 for data security should be factored into all business decision-making.¹²

9
10 51. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide*
11 *for Business*, which establishes guidelines for fundamental data security principles and practices
12 for business.¹³ Among other things, the guidelines note businesses should properly dispose of
13 personal information that is no longer needed; encrypt information stored on computer networks;
14 understand their network's vulnerabilities; and implement policies to correct security problems.
15 The guidelines also recommend that businesses use an intrusion detection system to expose a
16 breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone is
17 attempting to hack the system; watch for large amounts of data being transmitted from the system;
18 and have a response plan ready in the event of a breach.¹⁴

19
20
21 52. Additionally, the FTC recommends that companies limit access to sensitive data,
22 require complex passwords for network access, use industry-tested methods for security, monitor

23
24
25 ¹² *Start with Security: A Guide for Business*, FTC (June 2015),
<https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

26 ¹³ *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016),
<https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>.

27 ¹⁴ *Id.*

1 for suspicious activity on the network, and verify that third-party service providers have
2 implemented reasonable security measures.¹⁵

3 53. The FTC has brought enforcement actions against businesses for failing to
4 adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate
5 measures to protect against unauthorized access to confidential consumer data as an unfair act or
6 practice prohibited by Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §
7 45. Orders resulting from these actions further clarify the measures businesses must take to meet
8 their data security obligations.¹⁶

9
10 54. MGM also failed to comply with commonly accepted industry standards for data
11 security. Security standards commonly accepted among businesses that store PII using the internet
12 include, without limitation:

- 13 • Maintaining a secure firewall configuration;
- 14 • Maintaining appropriate design, systems, and controls to limit user access to certain
- 15 information as necessary;
- 16 • Monitoring for suspicious or irregular traffic to servers;
- 17 • Monitoring for suspicious credentials used to access servers;
- 18 • Monitoring for suspicious or irregular activity by known users;
- 19 • Monitoring for suspicious or unknown users;
- 20 • Monitoring for suspicious or irregular server requests;
- 21 • Monitoring for server requests for PII;
- 22
- 23
- 24

25
26 ¹⁵ See *Start with Security: A for Business*, FTC, *supra* n.12.

27 ¹⁶ See *Privacy and Security Enforcement Press Releases*, FTC, [https://www.ftc.gov/news-](https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement)
28 [events/media-resources/protecting-consumer-privacy/privacy-security-enforcement](https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement).

- 1 • Monitoring for server requests from VPNs; and
- 2 • Monitoring for server requests from Tor exit nodes.

3 55. MGM is also required by various states' laws and regulations to protect Plaintiffs'
4 and Class Members' PII and to handle any breach of the same in accordance with applicable breach
5 notification statutes.

6
7 56. In addition to its obligations under federal and state laws, MGM owed a duty to
8 Plaintiffs and Class Members whose PII were entrusted to MGM to exercise reasonable care in
9 obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from
10 being compromised, lost, stolen, accessed, and misused by unauthorized persons. MGM owed a
11 duty to Plaintiffs and Class Members to provide reasonable security, including consistency with
12 industry standards and requirements, and to ensure that its systems and networks adequately
13 protected the PII of Plaintiffs and Class Members.

14
15 57. MGM owed a duty to Plaintiffs and Class Members whose PII was entrusted to
16 MGM to design, maintain, and test its systems to ensure that the PII in MGM's possession was
17 adequately secured and protected.

18
19 58. MGM owed a duty to Plaintiffs and Class Members whose PII was entrusted to
20 MGM to create and implement reasonable data security practices and procedures to protect the PII
21 in its possession.

22
23 59. MGM owed a duty to Plaintiffs and Class Members whose PII was entrusted to
24 MGM to implement processes that would detect a breach on its data security systems in a timely
25 manner.

26
27 60. MGM owed a duty to Plaintiffs and Class Members whose PII was entrusted to
28 MGM to act upon data security warnings and alerts in a timely fashion.

1 61. MGM owed a duty to Plaintiffs and Class Members whose PII was entrusted to
2 MGM to disclose if its systems and data security practices were inadequate to safeguard
3 individuals' PII from theft because such an inadequacy would be a material fact in the decision to
4 entrust PII to MGM.

5
6 62. MGM owed a duty to Plaintiffs and Class Members whose PII was entrusted to
7 MGM to disclose in a timely and accurate manner when data breaches occurred.

8 63. MGM owed a duty of care to Plaintiffs and Class Members because they were
9 foreseeable and probable victims of any inadequacy in its affirmative development of the systems
10 to maintain PII and in its affirmative maintenance of those systems.

11 64. In this case, MGM was fully aware of its obligation to use reasonable measures to
12 protect the PII of its customers. MGM also knew it was a target for hackers. But despite
13 understanding the consequences of inadequate data security, MGM failed to comply with industry-
14 standard data security requirements.
15

16 ***The Effect of the Data Breach on Impacted Consumers***

17 65. The exponential cost to Plaintiffs and Class Members resulting from the Data
18 Breach cannot be overstated. Criminals can use victims' PII to open new financial accounts, incur
19 charges in credit, obtain governmental benefits and identifications, fabricate identities, and file
20 fraudulent tax returns well before a person whose PII was stolen becomes aware of it.¹⁷ Any one
21

22
23 ¹⁷ See *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity*
24 *Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737 (June 2007),
25 <https://www.gao.gov/new.items/d07737.pdf>; see also Melanie Lockert, *How do hackers use your*
26 *information for identity theft?*, CREDITKARMA (Oct. 1, 2021), [https://www.creditkarma.com/id-](https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information)
27 [theft/i/how-hackers-use-your-information](https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it); see also Ravi Sen, *Here's how much your personal*
28 *information is worth to cybercriminals – and what they do with it*, PBS (May 14, 2021),
[https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-](https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it)
[cybercriminals-and-what-they-do-with-it](https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it) (last visited Oct. 17, 2023); see also Alison Grace

1 of these instances of identity theft can have devastating consequences for the victim, causing years
2 of often irreversible damage to their credit scores, financial stability, and personal security.

3 66. Defendant was or should have been aware that it was collecting highly valuable
4 data, which has increasingly been the target of data breaches in recent years.

5 67. The link between a data breach and the risk of identity theft is simple and well
6 established. Criminals acquire and steal PII to monetize the information. Criminals monetize the
7 data by selling the stolen information on the black market to other criminals who then utilize the
8 information to commit a variety of identity theft related crimes discussed below.

9 68. The exposure of any PII can cause unexpected harms one would not ordinarily
10 associate with the type of information stolen. Cybercriminals routinely aggregate Private
11 Information from multiple illicit sources and use stolen information to gather even more
12 information through social engineering, credential stuffing, and other methods. The resulting
13 complete dossiers of PII are particularly prized among cybercriminals because they expose the
14 target to every manner of identity theft and fraud.

15 69. Identity thieves can use PII such as that exposed in the Data Breach to: (a) apply
16 for credit cards or loans (b) purchase prescription drugs or other medical services (c) commit
17 immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e)
18 obtain fraudulent government benefits or insurance benefits; (f) file a fraudulent tax return using
19 the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such
20 as obtaining a job, procuring housing, or giving false information to police during an arrest.

21
22
23
24
25
26
27

Johansen, *4 Lasting Effects of Identity Theft*, LIFELOCK BY NORTON (Feb. 4, 2021),
28 <https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-ofidentity-theft>.

1 ***Diminution of Value of PII***

2 70. PII is valuable property.¹⁸ Its value is axiomatic, considering the value of Big Data
3 in corporate America and that the consequences of cyber thefts include heavy prison sentences.
4 Even this obvious risk-to-reward analysis illustrates, beyond doubt, that PII has considerable
5 market value.

6
7 71. The PII stolen in the Data Breach is significantly more valuable than the loss of
8 credit card information in a large retailer data breach. Victims affected by those retailer breaches
9 could avoid much of the potential future harm by simply cancelling credit or debit cards and
10 obtaining replacements.

11 72. This type of data commands a much higher price on the dark web. As Martin Walter,
12 senior director at cybersecurity firm RedSeal, explained: “Compared to credit card information,
13 personally identifiable information ... [is] worth more than 10x on the black market.”¹⁹

14
15 73. Sensitive PII can sell for as much as \$363 per record according to the Infosec
16 Institute.²⁰

17 74. An active and robust legitimate marketplace for PII also exists. In 2019, the data
18 brokering industry was worth roughly \$200 billion.²¹ Indeed, a Social Security number, date of
19

20
21 ¹⁸ See *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity*
22 *Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737 (June 2007),
<https://www.gao.gov/new.items/d07737.pdf>, at 2.

23 ¹⁹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*
24 *Numbers*, (Feb. 6, 2015), [https://www.networkworld.com/article/2880366/anthem-hack-personal-](https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html)
[data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html](https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html).

25 ²⁰ See, e.g., John T. Soma, et al., *Corporate Privacy Trend: The “Value” of Personally*
26 *Identifiable Information (“Private Information”) Equals the “Value” of Financial Assets*, 15
27 *RICH. J.L. & TECH.* 11, at *3-4 (2009) (“Private Information, which companies obtain at little cost,
has quantifiable value that is rapidly reaching a level comparable to the value of traditional
financial assets.”) (citations omitted).

28 ²¹ David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, L.A.

1 birth, and full name can sell for \$60 to \$80 on the digital black market.²²

2 75. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an
3 inherent market value in both legitimate and dark markets, has been damaged and diminished by
4 its compromise and unauthorized release. However, this transfer of value occurred without any
5 consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss.
6 Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing
7 additional loss of value.
8

9 76. The fraudulent activity resulting from the Data Breach may not come to light for
10 years.

11 77. Plaintiffs and Class Members now face years of constant surveillance of their
12 financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are
13 incurring and will continue to incur such damages in addition to any fraudulent use of their PII.
14

15 78. Defendant was, or should have been, fully aware of the unique type and the
16 significant volume of data on Defendant's network, amounting to millions of individuals' detailed
17 PII and thus the significant number of individuals who would be harmed by the exposure of the
18 unencrypted data.

19 79. The injuries to Plaintiffs and Class Members were directly and proximately caused
20 by Defendant's failure to implement or maintain adequate data security measures for the PII of
21 Plaintiffs and Class Members.
22

23
24
25
26 TIMES (Nov. 5, 2019), <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.
27 ²² Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, PCMAG (Nov. 15,
28 2017), <https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web>.

1 ***Loss of Time to Mitigate the Risk of Identity Theft and Fraud***

2 80. As a result of the recognized risk of identity theft, when a data breach occurs and
3 an individual is notified by a company that their PII was compromised, as in this Data Breach, the
4 reasonable person is expected to take steps and spend time to address the dangerous situation, learn
5 about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud.
6 Failure to spend time taking steps to review accounts or credit reports could expose the individual
7 to greater financial harm.
8

9 81. Class Members have spent, and will spend, time on a variety of prudent actions, such
10 as researching and verifying the legitimacy of the Data Breach upon seeing news reports and
11 monitoring their credit reports and financial accounts for suspicious activity, as MGM advised in
12 its online notice.²³
13

14 82. These mitigation efforts are consistent with the U.S. Government Accountability
15 Office that released a report in 2007 regarding data breaches, in which it noted that victims of
16 identity theft will face “substantial costs and time to repair the damage to their good name and
17 credit record.”²⁴
18

19 83. Plaintiffs’ mitigation efforts are also consistent with the steps the FTC recommends
20 data breach victims take to protect their personal and financial information after a data breach,
21 including: contacting one of the credit bureaus to place a fraud alert (and considering an extended
22 fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports,
23 contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on
24

25
26

²³ See Notice of Data Breach, *supra* n.6.

27 ²⁴ See *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity*
28 *Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, *supra* n.18.

1 their credit, and correcting their credit reports.²⁵

2 84. Plaintiffs and Class Members now face years of constant surveillance of their
3 financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are
4 incurring and will continue to incur such damages in addition to any fraudulent use of their PII.
5

6 85. Defendant was, or should have been, fully aware of the unique type and the
7 significant volume of data on Defendant’s network, amounting to millions of individuals’ detailed
8 PII and, thus, the significant number of individuals who would be harmed by the exposure of the
9 unencrypted data.

10 86. The injuries to Plaintiffs and Class Members were directly and proximately caused
11 by Defendant’s failure to implement or maintain adequate data security measures for the PII of
12 Plaintiffs and Class Members.
13

14 ***Impact of Identity Theft Can Have Ripple Effects***

15 87. Reimbursing a consumer for a financial loss due to fraud does not make that
16 individual whole again. On the contrary, in addition to the irreparable damage that may result from
17 the theft of a Social Security number, identity theft victims must spend numerous hours and their
18 own money repairing the impact to their credit. The Department of Justice’s Bureau of Justice
19 Statistics found that identity theft victims “reported spending an average of about 7 hours clearing
20 up the issues” and resolving the consequences of fraud in 2014.
21

22 88. And, the impact of identity theft can have ripple effects, which can adversely affect
23 the future financial trajectories of victims’ lives. For example, the Identity Theft Resource Center
24 reports that respondents to their surveys in 2013-2016 described that the identity theft they
25

26
27 ²⁵ See *Identity Theft.gov*, FTC, <https://www.identitytheft.gov/Steps>.
28

1 experienced affected their ability to get credit cards and obtain loans such as student loans or
2 mortgages.²⁶ For some victims, this could mean the difference between going to college or not,
3 becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-
4 interest loan.

5 89. It is no wonder then that identity theft exacts a severe emotional toll on its victims.

6 90. The 2017 Identity Theft Resource Center survey²⁷ evidences the emotional
7 suffering experienced by victims of identity theft:
8

- 9
- 10 • 75% of respondents reported feeling severely distressed;
 - 11 • 67% reported anxiety;
 - 12 • 66% reported feelings of fear for the financial safety of family members;
 - 13 • 24% reported fear for their physical safety;
 - 14 • 15.2% reported that a relationship ended or was severely and negatively impacted
15 by the identity theft; and
 - 16 • 7% reported feeling suicidal.

17 91. Identity theft can also exact a physical toll on its victims. The same survey reported
18 that respondents experienced physical symptoms stemming from their experience with identity
19 theft:
20

- 21
- 22 • 48.3% of respondents reported sleep disturbances;
 - 23 • 37.1% reported an inability to concentrate and/or lack of focus;
 - 24 • 28.7% reported that they were unable to go to work because of physical symptoms;

25
26 ²⁶ Identity Theft Res. Ctr., *Identity Theft: The Aftermath 2017*, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf.

27 ²⁷ *Id.*

- 1 • 23.1% reported new physical illnesses, including aches and pains, heart
- 2 palpitations, sweating, and/or stomach issues;
- 3 • 12.6% reported a start or relapse into unhealthy or addictive behaviors.²⁸
- 4

5 92. There may also be a significant time lag between when PII is stolen and when it is
6 actually misused. According to the U.S. Government Accountability Office, which conducted a
7 study regarding data breaches:

8 [L]aw enforcement officials told us that in some cases, stolen data may be held for
9 up to a year or more before being used to commit identity theft. Further, once stolen
10 data have been sold or posted on the Web, fraudulent use of that information may
11 continue for years. As a result, studies that attempt to measure the harm resulting
12 from data breaches cannot necessarily rule out all future harm.²⁹

13 93. As the result of the Data Breach, Plaintiffs and Class Members have suffered and/or
14 will suffer or continue to suffer economic loss, a substantial risk of future identity theft, and other
15 actual harm for which they are entitled to damages, including, but not limited to, the following:

- 16 • Losing the inherent value of their PII;
- 17 • Losing the value of Defendant’s implicit promises of adequate data security;
- 18 • Identity theft and fraud resulting from the theft of their PII;
- 19 • Costs associated with the detection and prevention of identity theft and
20 unauthorized use of their PII;
- 21 • Costs associated with purchasing credit monitoring and identity theft protection
22 services;
- 23
- 24

25
26 ²⁸ *Id.*

27 ²⁹ *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft*
28 *Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, *supra* n.18.

- 1 • Unauthorized charges and loss of use of and access to their financial account funds
2 and costs associated with inability to obtain money from their accounts or being
3 limited in the amount of money they were permitted to obtain from their accounts,
4 including missed payments on bills and loans, late charges and fees, and adverse
5 effects on their credit;
- 6 • Lowered credit scores resulting from credit inquiries following fraudulent
7 activities;
- 8 • Costs associated with time spent and the loss of productivity or the enjoyment of
9 one's life from taking time to address and attempt to mitigate and address the actual
10 and future consequences of the Data Breach, including discovering fraudulent
11 charges, cancelling and reissuing cards, purchasing credit monitoring and identity
12 theft protection services, imposing withdrawal and purchase limits on compromised
13 accounts, and the stress, nuisance and annoyance of dealing with the repercussions
14 of the Data Breach; and
- 15 • The continued imminent and certainly impending injury flowing from potential
16 fraud and identity theft posed by their PII being in the possession of one or many
17 unauthorized third parties.

18 94. Additionally, Plaintiffs and Class Members place significant value in data security.

19 95. Because of the value consumers place on data privacy and security, companies with
20 robust data security practices can command higher prices than those who do not. Indeed, if
21 consumers did not value their data security and privacy, companies like Defendant would have no
22 reason to tout their data security efforts to their actual and potential customers.

23 96. Consequently, had consumers known the truth about Defendant's data security
24
25
26
27
28

1 practices—that Defendant would not adequately protect and store their data—they would not have
2 entrusted their PII to Defendant, purchased insurance that included Defendant’s services, or paid
3 as much for such services or benefits.

4 97. As such, Plaintiffs and Class Members did not receive the benefit of their bargain
5 with Defendant because they entrusted their PII and purchased accommodations, dining, gaming
6 and other goods and services with the reasonable expectation that Defendant would adequately
7 protect and store their data, which it did not.

8
9 **V. PLAINTIFFS’ EXPERIENCES**

10 ***Plaintiff Tonya Owens***

11 98. Plaintiff Tonya Owens (“Plaintiff Owens”) is a current MGM Rewards member.

12 99. In order to obtain an MGM Rewards membership, Plaintiff Owens was required to
13 provide her PII to Defendant, including her name, date of birth, contact information, and Social
14 Security number.

15 100. Upon information and belief, at the time of the Data Breach, Defendant retained
16 Plaintiff Owens’s PII in its system.

17 101. Plaintiff Owens is very careful about sharing her sensitive PII. Plaintiff stores any
18 documents containing her PII in a safe and secure location. She has never knowingly transmitted
19 unencrypted sensitive PII over the internet or any other unsecured source.

20 102. Plaintiff Owens would not have entrusted her PII to Defendant had she known of
21 Defendant’s lax data security policies.

22 103. As a result of the Data Breach, and at the direction of Defendant’s Notice, Plaintiff
23 Owens made reasonable efforts to mitigate the impact of the Data Breach, including researching
24 and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with
25
26
27
28

1 the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including
2 but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

3 104. Plaintiff Owens suffered actual injury from having her PII compromised as a result
4 of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost
5 or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
6 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
7 opportunity costs associated with attempting to mitigate the actual consequences of the Data
8 Breach; and (vii) the continued and certainly increased risk to her PII, which: (a) remains
9 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
10 backed up in Defendant’s possession and is subject to further unauthorized disclosures so long as
11 Defendant fails to undertake appropriate and adequate measures to protect the PII.
12

13 105. The Data Breach has caused Plaintiff Owens to suffer fear, anxiety, and stress,
14 which has been compounded by the fact that Defendant has still not fully informed her of key
15 details about the Data Breach’s occurrence.
16

17 106. As a result of the Data Breach, Plaintiff Owens anticipates spending considerable
18 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
19 Breach.
20

21 107. As a result of the Data Breach, Plaintiff Owens is at a present risk and will continue
22 to be at increased risk of identity theft and fraud for years to come.

23 108. Plaintiff Owens has a continuing interest in ensuring that her PII, which, upon
24 information and belief, remains backed up in Defendant’s possession, is protected and safeguarded
25 from future breaches.
26
27
28

1 ***Plaintiff Emily Kirwan***

2 109. Plaintiff Emily Kirwan (“Plaintiff Kirwan”) is a current MGM Rewards member.

3 110. In order to obtain an MGM Rewards membership, Plaintiff Kirwan was required to
4 provide her PII to Defendant, including her name, date of birth, contact information, and Social
5 Security number.
6

7 111. Upon information and belief, at the time of the Data Breach, Defendant retained
8 Plaintiff Kirwan’s PII in its system.

9 112. Plaintiff Kirwan is very careful about sharing her sensitive PII. Plaintiff stores any
10 documents containing her PII in a safe and secure location. She has never knowingly transmitted
11 unencrypted sensitive PII over the internet or any other unsecured source.
12

13 113. Plaintiff Kirwan would not have entrusted her PII to Defendant had she known of
14 Defendant’s lax data security policies.

15 114. As a result of the Data Breach, and at the direction of Defendant’s Notice, Plaintiff
16 Kirwan made reasonable efforts to mitigate the impact of the Data Breach, including changing her
17 debit card pin number and monitoring her financial accounts for fraudulent activity. Plaintiff
18 Kirwan has spent significant time dealing with the Data Breach—valuable time she otherwise
19 would have spent on other activities, including but not limited to work and/or recreation. This time
20 has been lost forever and cannot be recaptured.
21

22 115. Plaintiff Kirwan suffered actual injury from having her PII compromised as a result
23 of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost
24 or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
25 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
26 opportunity costs associated with attempting to mitigate the actual consequences of the Data
27
28

1 Breach; and (vii) the continued and certainly increased risk to her PII, which: (a) remains
2 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
3 backed up in Defendant’s possession and is subject to further unauthorized disclosures so long as
4 Defendant fails to undertake appropriate and adequate measures to protect the PII.
5

6 116. The Data Breach has caused Plaintiff Kirwan to suffer fear, anxiety, and stress,
7 which has been compounded by the fact that Defendant has still not fully informed her of key
8 details about the Data Breach’s occurrence.

9 117. As a result of the Data Breach, Plaintiff Kirwan anticipates spending considerable
10 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
11 Breach.

12 118. As a result of the Data Breach, Plaintiff Kirwan is at a present risk and will continue
13 to be at increased risk of identity theft and fraud for years to come.

14 119. Plaintiff Kirwan has a continuing interest in ensuring that her PII, which, upon
15 information and belief, remains backed up in Defendant’s possession, is protected and safeguarded
16 from future breaches.
17

18 ***Plaintiff David Zussman***

19 120. Plaintiff David Zussman (“Plaintiff Zussman”) is a current MGM Rewards
20 member.
21

22 121. In order to obtain an MGM Rewards membership, Plaintiff Zussman was required
23 to provide his PII to Defendant, including his name, date of birth, contact information, and Social
24 Security number.

25 122. Upon information and belief, at the time of the Data Breach, Defendant retained
26 Plaintiff Zussman’s PII in its system.
27
28

1 123. Plaintiff Zussman is very careful about sharing his sensitive PII. Plaintiff Zussman
2 stores any documents containing his PII in a safe and secure location. He has never knowingly
3 transmitted unencrypted sensitive PII over the internet or any other unsecured source.

4 124. Plaintiff Zussman would not have entrusted his PII to Defendant had he known of
5 Defendant's lax data security policies.
6

7 125. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff
8 Zussman made reasonable efforts to mitigate the impact of the Data Breach, including monitoring
9 his financial accounts for fraudulent activity. Plaintiff Zussman has spent significant time dealing
10 with the Data Breach—valuable time he otherwise would have spent on other activities, including
11 but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.
12

13 126. Plaintiff Zussman suffered actual injury from having his PII compromised as a
14 result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII;
15 (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting
16 to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
17 opportunity costs associated with attempting to mitigate the actual consequences of the Data
18 Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains
19 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
20 backed up in Defendant's possession and is subject to further unauthorized disclosures so long as
21 Defendant fails to undertake appropriate and adequate measures to protect the PII.
22

23 127. The Data Breach has caused Plaintiff Zussman to suffer fear, anxiety, and stress,
24 which has been compounded by the fact that Defendant has still not fully informed him of key
25 details about the Data Breach's occurrence.

26 128. As a result of the Data Breach, Plaintiff Zussman anticipates spending considerable
27
28

1 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
2 Breach.

3 129. As a result of the Data Breach, Plaintiff Zussman is at a present risk and will
4 continue to be at increased risk of identity theft and fraud for years to come.
5

6 130. Plaintiff Zussman has a continuing interest in ensuring that his PII, which, upon
7 information and belief, remains backed up in Defendant's possession, is protected and safeguarded
8 from future breaches.

9 ***Plaintiff David Lackey***

10 131. Plaintiff David Lackey ("Plaintiff Lackey") is a current MGM Rewards member.
11 He joined Defendant's rewards program over twenty years ago, and Plaintiff Lackey has, on
12 several occasions, visited MGM National Harbor in Oxon Hill, Maryland and also visits MGM
13 properties in Las Vegas, Nevada.
14

15 132. In order to obtain an MGM Rewards membership, Plaintiff Lackey was required to
16 provide his PII to Defendant, including his name, date of birth, contact information, and Social
17 Security number.

18 133. Upon information and belief, at the time of the Data Breach, Defendant retained
19 Plaintiff Lackey's PII in its system.
20

21 134. Plaintiff Lackey is very careful about sharing his sensitive PII. Plaintiff Lackey
22 stores any documents containing his PII in a safe and secure location. He has never knowingly
23 transmitted unencrypted sensitive PII over the internet or any other unsecured source.

24 135. Plaintiff Lackey would not have entrusted his PII to Defendant had he known of
25 Defendant's lax data security policies.

26 136. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff
27
28

1 Lackey made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Lackey has
2 spent significant time dealing with the Data Breach—valuable time he otherwise would have spent
3 on other activities, including but not limited to work and/or recreation. This time has been lost
4 forever and cannot be recaptured.

5
6 137. Further, as a result of the Data Breach, Plaintiff Lackey received increased text
7 phishing attempts from multiples sources in the weeks following the Data Breach.

8 138. Plaintiff Lackey suffered actual injury from having his PII compromised as a result
9 of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost
10 or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
11 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
12 opportunity costs associated with attempting to mitigate the actual consequences of the Data
13 Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains
14 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
15 backed up in Defendant’s possession and is subject to further unauthorized disclosures so long as
16 Defendant fails to undertake appropriate and adequate measures to protect the PII.

17
18 139. The Data Breach has caused Plaintiff Lackey to suffer fear, anxiety, and stress,
19 which has been compounded by the fact that Defendant has still not fully informed him of key
20 details about the Data Breach’s occurrence.

21
22 140. As a result of the Data Breach, Plaintiff Lackey anticipates spending considerable
23 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
24 Breach.

25 141. As a result of the Data Breach, Plaintiff Lackey is at a present risk and will continue
26 to be at increased risk of identity theft and fraud for years to come.

1 142. Plaintiff Lackey has a continuing interest in ensuring that his PII, which, upon
2 information and belief, remains backed up in Defendant’s possession, is protected and safeguarded
3 from future breaches.

4 ***Plaintiff Michael Pircio***

5
6 143. Plaintiff Michael Pircio (“Plaintiff Pircio”) is a current MGM Rewards member,
7 who last stayed at Defendant’s resorts in early September 2023.

8 144. In order to obtain an MGM Rewards membership, Plaintiff Pircio was required to
9 provide his PII to Defendant, including his name, date of birth, contact information, and Social
10 Security number.

11 145. Upon information and belief, at the time of the Data Breach, Defendant retained
12 Plaintiff Pircio’s PII in its system.

13
14 146. Plaintiff Pircio is very careful about sharing his sensitive PII. Plaintiff Pircio stores
15 any documents containing his PII in a safe and secure location. He has never knowingly transmitted
16 unencrypted sensitive PII over the internet or any other unsecured source.

17 147. Plaintiff Pircio would not have entrusted his PII to Defendant had he known of
18 Defendant’s lax data security policies.

19 148. As a result of the Data Breach, and at the direction of Defendant’s Notice, Plaintiff
20 Pircio made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Pircio has spent
21 significant time dealing with the Data Breach, including time spent verifying the legitimacy and
22 impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance
23 options; time spent self-monitoring his accounts with heightened scrutiny and time spent seeking
24 legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach-.
25 This is valuable time he otherwise would have spent on other activities, including but not limited
26
27
28

1 to work and/or recreation. This time has been lost forever and cannot be recaptured.

2 149. Plaintiff Pircio suffered actual injury from having his PII compromised as a result
3 of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost
4 or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
5 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
6 opportunity costs associated with attempting to mitigate the actual consequences of the Data
7 Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains
8 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
9 backed up in Defendant's possession and is subject to further unauthorized disclosures so long as
10 Defendant fails to undertake appropriate and adequate measures to protect the PII.
11

12 150. The Data Breach has caused Plaintiff Pircio to suffer fear, anxiety, and stress, which
13 has been compounded by the fact that Defendant has still not fully informed him of key details
14 about the Data Breach's occurrence.
15

16 151. As a result of the Data Breach, Plaintiff Pircio anticipates spending considerable
17 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
18 Breach.
19

20 152. As a result of the Data Breach, Plaintiff Pircio is at a present risk and will continue
21 to be at increased risk of identity theft and fraud for years to come.
22

23 153. Plaintiff Pircio has a continuing interest in ensuring that his PII, which, upon
24 information and belief, remains backed up in Defendant's possession, is protected and safeguarded
25 from future breaches.

26 ***Plaintiff David Terezo***

27 154. Plaintiff David Terezo ("Plaintiff Terezo") is a current MGM Rewards member.
28

1 155. In order to obtain an MGM Rewards membership, Plaintiff Terezo was required to
2 provide his PII to Defendant, including his name, date of birth, contact information, and Social
3 Security number.

4 156. Upon information and belief, at the time of the Data Breach, Defendant retained
5 Plaintiff Terezo's PII in its system.

6 157. Plaintiff Terezo is very careful about sharing his sensitive PII. Plaintiff Terezo
7 stores any documents containing his PII in a safe and secure location. He has never knowingly
8 transmitted unencrypted sensitive PII over the internet or any other unsecured source.

9 158. Plaintiff Terezo would not have entrusted his PII to Defendant had he known of
10 Defendant's lax data security policies.

11 159. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff
12 Terezo made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Terezo has
13 spent significant time dealing with the Data Breach, including changing his debit card pin number
14 and monitoring his financial accounts for fraudulent activity—valuable time he otherwise would
15 have spent on other activities, including but not limited to work and/or recreation. This time has
16 been lost forever and cannot be recaptured.

17 160. Plaintiff Terezo suffered actual injury from having his PII compromised as a result
18 of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost
19 or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
20 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
21 opportunity costs associated with attempting to mitigate the actual consequences of the Data
22 Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains
23 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
24
25
26
27
28

1 backed up in Defendant’s possession and is subject to further unauthorized disclosures so long as
2 Defendant fails to undertake appropriate and adequate measures to protect the PII.

3 161. The Data Breach has caused Plaintiff Terezo to suffer fear, anxiety, and stress,
4 which has been compounded by the fact that Defendant has still not fully informed him of key
5 details about the Data Breach’s occurrence.
6

7 162. As a result of the Data Breach, Plaintiff Terezo anticipates spending considerable
8 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
9 Breach.

10 163. As a result of the Data Breach, Plaintiff Terezo is at a present risk and will continue
11 to be at increased risk of identity theft and fraud for years to come.
12

13 164. Plaintiff Terezo has a continuing interest in ensuring that his PII, which, upon
14 information and belief, remains backed up in Defendant’s possession, is protected and safeguarded
15 from future breaches.

16 ***Plaintiff Ronald G. Rundell***

17 165. Plaintiff Ronald G. Rundell (“Plaintiff Rundell”) is a current MGM Rewards
18 member since before 2018.

19 166. In order to obtain an MGM Rewards membership, Plaintiff Rundell was required
20 to provide his PII to Defendant, including his name, date of birth, contact information, and Social
21 Security number.
22

23 167. Upon information and belief, at the time of the Data Breach, Defendant retained
24 Plaintiff Rundell’s PII in its system.

25 168. Plaintiff Rundell is very careful about sharing his sensitive PII. Plaintiff Rundell
26 stores any documents containing his PII in a safe and secure location. He has never knowingly
27
28

1 transmitted unencrypted sensitive PII over the internet or any other unsecured source.

2 169. Plaintiff Rundell would not have entrusted his PII to Defendant had he known of
3 Defendant's lax data security policies.

4 170. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff
5 Rundell made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Rundell has
6 spent significant time dealing with the Data Breach, including reviewing account statements and
7 monitoring credit reports—valuable time he otherwise would have spent on other activities,
8 including but not limited to work and/or recreation. This time has been lost forever and cannot be
9 recaptured.
10

11 171. Plaintiff Rundell suffered actual injury from having his PII compromised as a result
12 of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost
13 or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
14 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
15 opportunity costs associated with attempting to mitigate the actual consequences of the Data
16 Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains
17 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
18 backed up in Defendant's possession and is subject to further unauthorized disclosures so long as
19 Defendant fails to undertake appropriate and adequate measures to protect the PII.
20
21

22 172. The Data Breach has caused Plaintiff Rundell to suffer fear, anxiety, and stress,
23 which has been compounded by the fact that Defendant has still not fully informed him of key
24 details about the Data Breach's occurrence.

25 173. As a result of the Data Breach, Plaintiff Rundell anticipates spending considerable
26 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
27
28

1 Breach.

2 174. As a result of the Data Breach Plaintiff Rundell is at a present risk and will continue
3 to be at increased risk of identity theft and fraud for years to come.

4 175. Plaintiff Rundell has a continuing interest in ensuring that his PII, which, upon
5 information and belief, remains backed up in Defendant’s possession, is protected and safeguarded
6 from future breaches.

7
8 ***Plaintiff Paul Zari***

9 176. Plaintiff Paul Zari (“Plaintiff Zari”) is a current MGM Rewards member.

10 177. In order to obtain an MGM Rewards membership, Plaintiff Zari was required to
11 provide his PII to Defendant, including his name, date of birth, contact information, and Social
12 Security number.

13 178. Upon information and belief, at the time of the Data Breach, Defendant retained
14 Plaintiff Zari’s PII in its system.

15 179. Plaintiff Zari is very careful about sharing his sensitive PII. Plaintiff Zari stores any
16 documents containing his PII in a safe and secure location. He has never knowingly transmitted
17 unencrypted sensitive PII over the internet or any other unsecured source.

18 180. Plaintiff Zari would not have entrusted his PII to Defendant had he known of
19 Defendant’s lax data security policies.

20 181. As a result of the Data Breach, and at the direction of Defendant’s Notice, Plaintiff
21 Zari made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Zari has spent
22 significant time dealing with the Data Breach—valuable time he otherwise would have spent on
23 other activities, including but not limited to work and/or recreation. This time has been lost forever
24 and cannot be recaptured.
25
26
27
28

1 182. Plaintiff Zari suffered actual injury from having his PII compromised as a result of
2 the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or
3 diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate
4 the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity
5 costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii)
6 the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available
7 for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's
8 possession and is subject to further unauthorized disclosures so long as Defendant fails to
9 undertake appropriate and adequate measures to protect the PII.
10

11 183. The Data Breach has caused Plaintiff Zari to suffer fear, anxiety, and stress, which
12 has been compounded by the fact that Defendant has still not fully informed him of key details
13 about the Data Breach's occurrence.
14

15 184. As a result of the Data Breach, Plaintiff Zari anticipates spending considerable time
16 and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

17 185. As a result of the Data Breach, Plaintiff Zari is at a present risk and will continue
18 to be at increased risk of identity theft and fraud for years to come.

19 186. Plaintiff Zari has a continuing interest in ensuring that his PII, which, upon
20 information and belief, remains backed up in Defendant's possession, is protected and safeguarded
21 from future breaches.
22

23 ***Plaintiff Michael Manson***

24 187. Plaintiff Michael Manson ("Plaintiff Manson") is a current MGM Rewards
25 member.

26 188. In order to obtain an MGM Rewards membership, Plaintiff Manson was required
27
28

1 to provide his PII to Defendant, including his name, date of birth, contact information, and Social
2 Security number.

3 189. Upon information and belief, at the time of the Data Breach, Defendant retained
4 Plaintiff Manson's PII in its system.

5 190. Plaintiff Manson is very careful about sharing his sensitive PII. Plaintiff Manson
6 stores any documents containing his PII in a safe and secure location. He has never knowingly
7 transmitted unencrypted sensitive PII over the internet or any other unsecured source.
8

9 191. Plaintiff Manson would not have entrusted his PII to Defendant had he known of
10 Defendant's lax data security policies.

11 192. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff
12 Manson made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Manson has
13 spent significant time dealing with the Data Breach—valuable time he otherwise would have spent
14 on other activities, including but not limited to work and/or recreation. This time has been lost
15 forever and cannot be recaptured.
16

17 193. Plaintiff Manson suffered actual injury from having his PII compromised as a result
18 of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost
19 or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
20 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
21 opportunity costs associated with attempting to mitigate the actual consequences of the Data
22 Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains
23 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
24 backed up in Defendant's possession and is subject to further unauthorized disclosures so long as
25 Defendant fails to undertake appropriate and adequate measures to protect the PII.
26
27
28

1 194. The Data Breach has caused Plaintiff Manson to suffer fear, anxiety, and stress,
2 which has been compounded by the fact that Defendant has still not fully informed him of key
3 details about the Data Breach’s occurrence.

4 195. As a result of the Data Breach, Plaintiff Manson anticipates spending considerable
5 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
6 Breach.

7 196. As a result of the Data Breach, Plaintiff Manson is at a present risk and will continue
8 to be at increased risk of identity theft and fraud for years to come.

9 197. Plaintiff Manson has a continuing interest in ensuring that his PII, which, upon
10 information and belief, remains backed up in Defendant’s possession, is protected and safeguarded
11 from future breaches.
12

13 ***Plaintiff Kyle Sloan***
14

15 198. Plaintiff Kyle Sloan (“Plaintiff Sloan”) is a current MGM Rewards member since
16 December 2021.

17 199. In order to obtain an MGM Rewards membership, Plaintiff Sloan was required to
18 provide his PII to Defendant, including his name, date of birth, contact information, and Social
19 Security number.
20

21 200. Upon information and belief, at the time of the Data Breach, Defendant retained
22 Plaintiff Sloan’s PII in its system.

23 201. Plaintiff Sloan is very careful about sharing his sensitive PII. Plaintiff Sloan stores
24 any documents containing his PII in a safe and secure location. He has never knowingly transmitted
25 unencrypted sensitive PII over the internet or any other unsecured source.

26 202. Plaintiff Sloan would not have entrusted his PII to Defendant had he known of
27
28

1 Defendant's lax data security policies.

2 203. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff
3 Sloan made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Sloan has spent
4 significant time dealing with the Data Breach, including self-monitoring accounts and credit
5 reports to ensure no fraudulent activity has occurred, such as checking his bank accounts and credit
6 cards every day to look for unauthorized or suspicious activity, and checking his Experian ID theft
7 monitoring account routinely since the Data Breach. This is valuable time he otherwise would have
8 spent on other activities, including but not limited to work and/or recreation. This time has been
9 lost forever and cannot be recaptured.
10

11 204. Plaintiff Sloan suffered actual injury from having his PII compromised as a result
12 of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost
13 or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
14 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
15 opportunity costs associated with attempting to mitigate the actual consequences of the Data
16 Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains
17 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
18 backed up in Defendant's possession and is subject to further unauthorized disclosures so long as
19 Defendant fails to undertake appropriate and adequate measures to protect the PII.
20
21

22 205. Further, Plaintiff Sloan has noticed an increase in spam calls since the Data Breach.

23 206. The Data Breach has caused Plaintiff Sloan to suffer fear, anxiety, and stress, which
24 has been compounded by the fact that Defendant has still not fully informed him of key details
25 about the Data Breach's occurrence.

26 207. As a result of the Data Breach, Plaintiff Sloan anticipates spending considerable
27
28

1 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
2 Breach.

3 208. As a result of the Data Breach, Plaintiff Sloan is at a present risk and will continue
4 to be at increased risk of identity theft and fraud for years to come.

5 209. Plaintiff Sloan has a continuing interest in ensuring that his PII, which, upon
6 information and belief, remains backed up in Defendant's possession, is protected and safeguarded
7 from future breaches.

8
9 ***Plaintiff Michelle Righetti***

10 210. Plaintiff Michelle Righetti ("Plaintiff Righetti") is a current MGM customer.

11 211. In order to receive Defendant's services, Plaintiff Righetti was required to provide
12 her PII to Defendant, including her name, date of birth, contact information, and Social Security
13 number.

14 212. Upon information and belief, at the time of the Data Breach, Defendant retained
15 Plaintiff Righetti's PII in its system.

16 213. Plaintiff Righetti is very careful about sharing her sensitive PII. Plaintiff Righetti
17 stores any documents containing her PII in a safe and secure location. She has never knowingly
18 transmitted unencrypted sensitive PII over the internet or any other unsecured source.

19 214. Plaintiff Righetti would not have entrusted her PII to Defendant had she known of
20 Defendant's lax data security policies.

21 215. As a result of the Data Breach, and at the direction of Defendant's Notice, Plaintiff
22 Righetti made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Righetti has
23 spent significant time dealing with the Data Breach—valuable time she otherwise would have spent
24 on other activities, including but not limited to work and/or recreation. This time has been lost
25
26
27
28

1 forever and cannot be recaptured.

2 216. Plaintiff Righetti suffered actual injury from having her PII compromised as a result
3 of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost
4 or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
5 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
6 opportunity costs associated with attempting to mitigate the actual consequences of the Data
7 Breach; and (vii) the continued and certainly increased risk to her PII, which: (a) remains
8 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
9 backed up in Defendant’s possession and is subject to further unauthorized disclosures so long as
10 Defendant fails to undertake appropriate and adequate measures to protect the PII.
11

12 217. The Data Breach has caused Plaintiff Righetti to suffer fear, anxiety, and stress,
13 which has been compounded by the fact that Defendant has still not fully informed her of key
14 details about the Data Breach’s occurrence.
15

16 218. As a result of the Data Breach, Plaintiff Righetti anticipates spending considerable
17 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
18 Breach.
19

20 219. As a result of the Data Breach, Plaintiff Righetti is at a present risk and will continue
21 to be at increased risk of identity theft and fraud for years to come.
22

23 220. Plaintiff Righetti has a continuing interest in ensuring that her PII, which, upon
24 information and belief, remains backed up in Defendant’s possession, is protected and safeguarded
25 from future breaches.

26 ***Plaintiff Edgar Mejia***

27 221. Plaintiff Edgar Mejia (“Plaintiff Mejia”) is a current MGM customer.
28

1 222. In order to receive Defendant’s services, Plaintiff Mejia was required to provide his
2 PII to Defendant, including his name, date of birth, contact information, and Social Security
3 number.

4 223. Upon information and belief, at the time of the Data Breach, Defendant retained
5 Plaintiff Mejia’s PII in its system.

6 224. Plaintiff Mejia is very careful about sharing his sensitive PII. Plaintiff Mejia stores
7 any documents containing his PII in a safe and secure location. He has never knowingly transmitted
8 unencrypted sensitive PII over the internet or any other unsecured source.

9 225. Plaintiff Mejia would not have entrusted his PII to Defendant had he known of
10 Defendant’s lax data security policies.

11 226. As a result of the Data Breach, and at the direction of Defendant’s Notice, Plaintiff
12 Mejia made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff Mejia has spent
13 significant time dealing with the Data Breach—this is valuable time he otherwise would have spent
14 on other activities, including but not limited to work and/or recreation. This time has been lost
15 forever and cannot be recaptured.

16 227. Plaintiff Mejia suffered actual injury from having his PII compromised as a result
17 of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost
18 or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
19 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
20 opportunity costs associated with attempting to mitigate the actual consequences of the Data
21 Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains
22 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
23 backed up in Defendant’s possession and is subject to further unauthorized disclosures so long as
24
25
26
27
28

1 Defendant fails to undertake appropriate and adequate measures to protect the PII.

2 228. The Data Breach has caused Plaintiff Mejia to suffer fear, anxiety, and stress, which
3 has been compounded by the fact that Defendant has still not fully informed him of key details
4 about the Data Breach’s occurrence.

5 229. As a result of the Data Breach, Plaintiff Mejia anticipates spending considerable
6 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
7 Breach.

8 230. As a result of the Data Breach, Plaintiff Mejia is at a present risk and will continue
9 to be at increased risk of identity theft and fraud for years to come.

10 231. Plaintiff Mejia has a continuing interest in ensuring that his PII, which, upon
11 information and belief, remains backed up in Defendant’s possession, is protected and safeguarded
12 from future breaches.

13 ***Plaintiff DuJun Johnson***

14 232. Plaintiff DuJun Johnson (“Plaintiff D. Johnson”) is a current MGM customer.

15 233. In order to receive Defendant’s services, Plaintiff D. Johnson was required to
16 provide his PII to Defendant, including his name, date of birth, contact information, and Social
17 Security number.

18 234. Upon information and belief, at the time of the Data Breach, Defendant retained
19 Plaintiff D. Johnson’s PII in its system.

20 235. Plaintiff D. Johnson is very careful about sharing his sensitive PII. Plaintiff D.
21 Johnson stores any documents containing his PII in a safe and secure location. He has never
22 knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

23 236. Plaintiff D. Johnson would not have entrusted his PII to Defendant had he known
24
25
26
27
28

1 of Defendant’s lax data security policies.

2 237. As a result of the Data Breach, and at the direction of Defendant’s Notice, Plaintiff
3 D. Johnson made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff D. Johnson
4 has spent significant time dealing with the Data Breach—this is valuable time he otherwise would
5 have spent on other activities, including but not limited to work and/or recreation. This time has
6 been lost forever and cannot be recaptured.

7
8 238. Plaintiff D. Johnson suffered actual injury from having his PII compromised as a
9 result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii)
10 lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to
11 mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost
12 opportunity costs associated with attempting to mitigate the actual consequences of the Data
13 Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains
14 unencrypted and available for unauthorized third parties to access and abuse; and (b) remains
15 backed up in Defendant’s possession and is subject to further unauthorized disclosures so long as
16 Defendant fails to undertake appropriate and adequate measures to protect the PII.

17
18 239. The Data Breach has caused Plaintiff D. Johnson to suffer fear, anxiety, and stress,
19 which has been compounded by the fact that Defendant has still not fully informed him of key
20 details about the Data Breach’s occurrence.

21
22 240. As a result of the Data Breach, Plaintiff D. Johnson anticipates spending
23 considerable time and money on an ongoing basis to try to mitigate and address harms caused by
24 the Data Breach.

25 241. As a result of the Data Breach, Plaintiff D. Johnson is at a present risk and will
26 continue to be at increased risk of identity theft and fraud for years to come.

1 242. Plaintiff D. Johnson has a continuing interest in ensuring that his PII, which, upon
2 information and belief, remains backed up in Defendant’s possession, is protected and safeguarded
3 from future breaches.

4
5 **VI. CLASS ACTION ALLEGATIONS**

6 243. Plaintiffs bring this action on behalf of himself and the members of the proposed
7 Class, which consists of:

8 **Nationwide Class:** All persons in the United States whose Private Information was
9 accessed during the Data Breach.

10 **California Subclass:** All persons in California whose Private Information was
11 accessed during the Data Breach.

12 244. Excluded from the Class are Defendant, any entity in which Defendant has a
13 controlling interest, and Defendant’s officers, directors, legal representatives, successors,
14 subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer
15 presiding over this matter and members of their immediate families and judicial staff.

16 245. Plaintiffs reserve the right to amend the above definition or to propose subclasses
17 before the Court determines whether certification is appropriate.

18 246. **Numerosity:** The proposed Class is so numerous that joinder of all members is
19 impracticable. Based on informal discovery, the Class is believed to be approximately seventy-
20 five million individuals.

21 247. **Typicality:** Plaintiffs’ claims are typical of the claims of the Class. Plaintiffs and
22 all members of the Class were injured through Defendant’s uniform misconduct. The same event
23 and conduct that gave rise to Plaintiffs’ claims are identical to those that give rise to the claims of
24 every other Class member because Plaintiffs and each member of the Class had their sensitive PII
25 compromised in the same way by the same conduct of Defendant.
26
27
28

1 248. **Adequacy:** Plaintiffs is an adequate representative of the Class because Plaintiffs’
2 interests do not conflict with the interests of the Class; Plaintiffs has retained competent counsel
3 who are experienced in prosecuting complex class action and data breach class action litigation;
4 and Plaintiffs and Plaintiffs’ counsel intend to prosecute this action vigorously. The interests of
5 the Class will be fairly and adequately protected by Plaintiffs and their counsel.
6

7 249. **Superiority:** A class action is superior to all other available methods for the fair
8 and efficient adjudication of this lawsuit because individual litigation of the claims of all members
9 of the Class is economically unfeasible and procedurally impracticable. The injury suffered by
10 each individual member of the Class is relatively small in comparison to the burden and expense
11 of individual prosecution of litigation. It would be very difficult for members of the Class to
12 effectively redress Defendant’s wrongdoing. Further, individualized litigation presents a potential
13 for inconsistent or contradictory judgments.
14

15 250. **Commonality and Predominance:** There are numerous questions of law and fact
16 common to the Class which predominate over any questions affecting only individual members of
17 the Class.

18 251. Among the questions of law and fact common to the Class are:

- 19 a. Whether Defendant engaged in the wrongful conduct alleged herein;
20 b. Whether Defendant failed to adequately safeguard Plaintiffs’ and the Class’s PII;
21 c. Whether Defendant negligently hired and/or failed to supervise the third-party
22 vendor it hired and gave access to Plaintiffs’ and the Class’s PII;
23 d. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect
24 their PII, and whether it breached this duty;
25 e. Whether Defendant breached its duties to Plaintiffs and the Class as a result of the
26
27
28

1 Data Breach;

2 f. Whether Defendant’s conduct, including its failure to act, resulted in or was the
3 proximate cause of the breach;

4 g. Whether Defendant was negligent in permitting the third-party access to
5 Plaintiffs’ and the Class’s PII;

6 h. Whether Defendant was negligent in failing to adhere to reasonable retention
7 policies, thereby greatly increasing the size of the Data Breach;

8 i. Whether Defendant failed to adequately respond to the Data Breach, including
9 failing to investigate it diligently and notify affected individuals in the most
10 expedient time possible and without unreasonable delay, and whether this caused
11 damages to Plaintiffs and the Class;

12 j. Whether Defendant continues to breach duties to Plaintiffs and the Class;

13 k. Whether Plaintiffs and the Class suffered injury as a proximate result of
14 Defendant’s negligent actions or failures to act;

15 l. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief,
16 and other relief; and

17 m. Whether Defendant’s actions alleged herein constitute gross negligence, and
18 whether Plaintiffs and Class Members are entitled to punitive damages.
19
20
21

22 **VII. COUNTS**

23 **FIRST CAUSE OF ACTION**
24 **NEGLIGENCE**
25 **(By Plaintiffs and on Behalf of the Class)**

26 252. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth
27 above and incorporate them at this point by reference as though set forth in full.

28 253. Defendant owed a duty of care to Plaintiffs and Class Members to use reasonable

1 means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure,
2 to guard it from theft, and to detect any attempted or actual breach of its systems, as alleged herein.
3 These common law duties existed because Plaintiffs and Class Members were the foreseeable and
4 probable victims of any inadequate security practices in Defendant's affirmative development and
5 maintenance of its data security systems and its hiring of third-party providers entrusted with
6 accessing, storing, safeguarding, handling, collecting, and/or protecting Plaintiffs' and Class
7 Members' PII. In fact, not only was it foreseeable that Defendant and Class Members would be
8 harmed by the failure to protect their PII because hackers routinely attempt to steal such
9 information and use it for nefarious purposes, Defendant also knew that it was more likely than
10 not that Plaintiffs and other Class Members would be harmed by such exposure and theft of their
11 PII.
12

13
14 254. Defendant's duties to use reasonable security measures also arose because of a
15 special relationship with Plaintiffs and Class Members because of being entrusted with their PII,
16 which provided an independent duty of care. Plaintiffs' and Class Members' willingness to entrust
17 Defendant with their PII was predicated on the understanding that Defendant would take adequate
18 security precautions. Moreover, Defendant could protect its network and systems, and the PII it
19 stored on them, from unauthorized access.
20

21 255. Defendant's duties to use reasonable data security measures also arose under
22 Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting
23 commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use
24 reasonable measures to protect PII. Various FTC publications and data security breach orders
25 further form the basis of Defendant's duties.
26

27 256. Defendant breached the aforementioned duties when it failed to use security
28

1 practices that would protect the PII provided to it by Plaintiffs and Class Members, thus resulting
2 in unauthorized exposure and access to Plaintiffs' and Class Members' PII.

3 257. Defendant further breached the aforementioned duties by failing to design, adopt,
4 implement, control, manage, monitor, update, and audit its processes, controls, policies,
5 procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiffs'
6 and Class Members' PII within its possession, custody, and control.

7 258. As a direct and proximate cause of Defendant's failure to use appropriate security
8 practices and failure to select a third-party provider with adequate data security measures,
9 Plaintiffs' and Class Members' PII was exposed, disseminated, and made available to unauthorized
10 third parties.

11 259. Defendant admitted that Plaintiffs' and Class Members' PII was wrongfully
12 disclosed as a result of the Data Breach.

13 260. The Data Breach caused direct and substantial damages to Plaintiffs and Class
14 Members, as well as the likelihood of future and imminent harm through the dissemination of their
15 PII and the greatly enhanced risk of credit fraud and identity theft.

16 261. By engaging in the foregoing acts and omissions, Defendant committed the
17 common law tort of negligence. For all the reasons stated above, Defendant's conduct was
18 negligent and departed from reasonable standards of care including by, but not limited to failing
19 to adequately limit access to and protect the PII; failing to conduct regular security audits; and
20 failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and
21 Class Members' PII.

22 262. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs
23 and Class Members, their PII would not have been compromised.

1 263. Neither Plaintiffs nor Class Members contributed to the Data Breach or subsequent
2 misuse of their PII as described in this Complaint.

3 264. As a direct and proximate result of Defendant’s negligence, Plaintiffs and Class
4 Members have been injured and are entitled to damages in an amount to be proven at trial. Such
5 injuries include one or more of the following: ongoing, imminent, certainly impending threat of
6 identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual
7 identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss
8 of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the
9 compromised PII on the black market; mitigation expenses and time spent on credit monitoring,
10 identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach
11 investigating the nature of the Data Breach not fully disclosed by Defendant, reviewing bank
12 statements, payment card statements, and credit reports; expenses and time spent initiating fraud
13 alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their
14 bargains and overcharges for services; and other economic and non-economic harm.
15
16

17
18 **SECOND CAUSE OF ACTION**
19 **NEGLIGENCE *PER SE***
20 **(By Plaintiffs and on Behalf of the Class)**

21 265. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth
22 above and incorporate them at this point by reference as though set forth in full.

23 266. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or
24 affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice
25 by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and
26 orders also form the basis of Defendant’s duty.

27 267. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing
28

1 to use reasonable measures to protect PII and not complying with industry standards. Defendant's
2 conduct was particularly unreasonable given the nature and amount of PII obtained and stored and
3 the foreseeable consequences of a data breach.

4 268. Defendant's violation of Section 5 of the FTC Act (and similar state statutes)
5 constitutes negligence *per se*.

6 269. Plaintiffs and Class Members are consumers within the class of persons Section 5
7 of the FTC Act (and similar state statutes) were intended to protect.

8 270. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar
9 state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement
10 actions against businesses which, as a result of Defendant's failure to employ reasonable data
11 security measures and avoid unfair and deceptive practices, caused the same harm suffered by
12 Plaintiffs and Class Members.

13 271. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class
14 Members have been injured and are entitled to damages in an amount to be proven at trial. Such
15 injuries include one or more of the following: ongoing, imminent, certainly impending threat of
16 identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual
17 identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss
18 of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the
19 compromised PII on the black market; mitigation expenses and time spent on credit monitoring,
20 identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach
21 investigating the nature of the Data Breach not fully disclosed by Defendant, reviewing bank
22 statements, payment card statements, and credit reports; expenses and time spent initiating fraud
23 alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their
24
25
26
27
28

1 bargains and overcharges for services; and other economic and non-economic harm.

2 **THIRD CAUSE OF ACTION**
3 **BREACH OF IMPLIED CONTRACT**
4 **(By Plaintiffs and on Behalf of the Class)**

5 272. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth
6 above and incorporate them at this point by reference as though set forth in full.

7 273. Plaintiffs and Class Members entered into an implied contract with MGM when
8 they obtained products or services from MGM, joined the loyalty program, or otherwise provided
9 PII to MGM.

10 274. As part of these transactions, MGM agreed to safeguard and protect the PII of
11 Plaintiffs and Class Members and to timely and accurately notify them if their PII was breached
12 or compromised.

13 275. Plaintiffs and Class Members entered into the implied contracts with the reasonable
14 expectation that MGM's data security practices and policies were reasonable and consistent with
15 legal requirements and industry standards. Plaintiffs and Class Members believed that MGM
16 would use part of the monies paid to MGM under the implied contracts or the monies obtained
17 from the benefits derived from the PII they provided to fund proper and reasonable data security
18 practices.

19 276. Plaintiffs and Class Members would not have provided and entrusted their PII to
20 MGM or would have paid less for MGM products or services in the absence of the implied contract
21 or implied terms between them and MGM. The safeguarding of the PII of Plaintiffs and Class
22 Members was critical to realize the intent of the parties.

23 277. Plaintiffs and Class Members fully performed their obligations under the implied
24 contracts with MGM.

1 278. MGM breached its implied contracts with Plaintiffs and Class Members to protect
2 their PII when it (1) failed to take reasonable steps to use safe and secure systems to protect that
3 information; and (2) disclosed that information to unauthorized third parties.

4 279. As a direct and proximate result of MGM's breach of implied contract, Plaintiffs
5 and Class Members have been injured and are entitled to damages in an amount to be proven at
6 trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending
7 threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic
8 harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic
9 harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the
10 compromised PII on the black market; mitigation expenses and time spent on credit monitoring,
11 identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach
12 reviewing bank statements, credit card statements, and credit reports, among other related
13 activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost
14 work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality
15 identity defense and credit monitoring services made necessary as mitigation measures because of
16 MGM's Data Breach; lost benefit of their bargains and overcharges for services or products;
17 nominal and general damages; and other economic and non-economic harm.
18
19
20

21 **FOURTH CAUSE OF ACTION**
22 **UNJUST ENRICHMENT**
23 **(In the alternative)**
24 **(By Plaintiffs and on Behalf of the Class)**

25 280. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth
26 above and incorporate them at this point by reference as though set forth in full.

27 281. This claim is pleaded in the alternative to the Breach of Implied contract claim set
28 forth in the Third Cause of Action.

1 282. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII
2 about them that was conferred upon, collected by, and maintained by Defendant and that was
3 ultimately stolen in the Data Breach.

4 283. Defendant benefitted from the conferral upon it of the PII pertaining to Plaintiffs
5 and Class Members and by its ability to retain, use, sell, and profit from that information. MGM
6 understood that it was in fact so benefitted.

7 284. MGM also understood and appreciated that the PII pertaining to Plaintiffs and Class
8 Members was private and confidential and its value depended upon MGM maintaining the privacy
9 and confidentiality of that PII.

10 285. But for MGM's willingness and commitment to maintain its privacy and
11 confidentiality, Plaintiffs and Class Members would not have provided their PII to MGM or would
12 not have permitted MGM to gather additional PII.

13 286. Plaintiffs' and Class Members' PII has an independent value to MGM.

14 287. MGM admits that it uses the PII it collects for, among other things, "recording and
15 accessing gaming-related activity," "customizing [customers] experience while visiting, using
16 and/or accessing MGM Online Services and/or MGM Resorts," "protecting and defending MGM
17 Resorts International and its affiliates against legal actions or claims," "satisfying contractual
18 obligations," "assess[ing] and improv[ing] [its] products and services," and "conducting internal
19 research, analytics, and statistical or demographic analysis."³⁰

20 288. Because of its use of Plaintiffs' and Class Members' PII, MGM sold more services
21 and products than it otherwise would have. MGM was unjustly enriched by profiting from the
22

23
24
25
26
27 ³⁰ Privacy Policy, MGM (July 10, 2023), <https://www.mgmresorts.com/en/privacy-policy.html>.

1 additional services and products it was able to market, sell, and create through the use of Plaintiffs’
2 and Class Members’ PII to the detriment of Plaintiffs and Class Members.

3 289. MGM also benefitted through its unjust conduct by retaining money paid by
4 Plaintiffs and Class Members that it should have used to provide proper data security to protect
5 Plaintiffs’ and Class Members’ PII.
6

7 290. It is inequitable for MGM to retain these benefits.

8 291. As a result of MGM’S wrongful conduct as alleged in this Complaint (including
9 among other things its failure to employ proper data security measures, its continued maintenance
10 and use of the PII belonging to Plaintiffs and Class Members without having proper data security
11 measures, and its other conduct facilitating the theft of that PII), MGM has been unjustly enriched
12 at the expense of, and to the detriment of, Plaintiffs and Class Members.
13

14 292. MGM’S unjust enrichment is traceable to, and resulted directly and proximately
15 from, the conduct alleged herein, including the compiling and use of Plaintiffs’ and Class
16 Members’ sensitive PII, while at the same time failing to maintain that information secure from
17 intrusion and theft by hackers and identity thieves.

18 293. It is inequitable, unfair, and unjust for MGM to retain these wrongfully obtained
19 benefits. MGM’S retention of wrongfully obtained monies would violate fundamental principles
20 of justice, equity, and good conscience.
21

22 294. The benefit conferred upon, received, and enjoyed by MGM was not conferred
23 officiously or gratuitously, and it would be inequitable, unfair, and unjust for MGM to retain the
24 benefit.

25 295. MGM’S defective security and its unfair and deceptive conduct have, among other
26 things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to
27
28

1 mitigate and monitor the use of their PII and has caused the Plaintiffs and Class Members other
2 damages as described herein.

3 296. Plaintiffs have no adequate remedy at law.

4 297. MGM is therefore liable to Plaintiffs and Class Members for restitution or
5 disgorgement in the amount of the benefit conferred on MGM as a result of its wrongful conduct,
6 including specifically: the value to MGM of the PII that was stolen in the Data Breach; the profits
7 MGM received and is receiving from the use of that information; the amounts that MGM
8 overcharged Plaintiffs and Class Members for use of MGM's products and services; and the
9 amounts that MGM should have spent to provide proper data security to protect Plaintiffs' and
10 Class Members' PII.
11

12 **FIFTH CAUSE OF ACTION**
13 **BREACH OF CONFIDENCE**
14 **(By Plaintiffs and on Behalf of the Class)**

15 298. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth
16 above and incorporate them at this point by reference as though set forth in full.

17 299. Plaintiffs and Class Members maintained a confidential relationship with MGM
18 whereby MGM undertook a duty not to disclose to unauthorized parties the PII that Plaintiffs and
19 Class Members provide to MGM. Such PII was confidential and novel, highly personal and
20 sensitive, and not generally known.
21

22 300. MGM knew Plaintiffs' and Class Members' PII was disclosed in confidence and
23 understood the confidence was to be maintained, including by expressly and implicitly agreeing
24 to protect the confidentiality and security of the PII it collected, stored, and maintained.

25 301. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs'
26 and Class Members' PII in violation of this understanding. The unauthorized disclosure occurred
27
28

1 because MGM failed to implement and maintain reasonable safeguards to protect the PII in its
2 possession and failed to comply with industry-standard data security practices.

3 302. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of
4 their confidential information to an unauthorized third party.

5 303. But for MGM'S actions and inactions in violation of the parties' understanding of
6 confidence, the PII of Plaintiffs and Class Members would not have been compromised, stolen,
7 viewed, accessed, and used by unauthorized third parties. MGM'S actions and inaction were the
8 direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting
9 damages.
10

11 304. The injury and harm Plaintiffs and Class Members suffered was the reasonably
12 foreseeable result of MGM'S unauthorized disclosure of Plaintiffs' and Class Members' PII.
13 MGM knew its computer systems and technologies for accepting, securing, and storing Plaintiffs'
14 and Class Members' PII had serious security vulnerabilities because MGM failed to observe even
15 basic information security practices or correct known security vulnerabilities.
16

17 305. As a direct and proximate result of MGM'S breach of confidence, Plaintiffs and
18 Class Members have been injured and are entitled to damages in an amount to be proven at trial.
19 Such injuries include one or more of the following: ongoing, imminent, certainly impending threat
20 of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm;
21 actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm;
22 loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the
23 compromised PII on the black market; mitigation expenses and time spent on credit monitoring,
24 identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach
25 reviewing bank statements, credit card statements, and credit reports, among other related
26
27
28

1 activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost
2 work time; lost value of the PII; the amount of the actuarial present value of ongoing high-quality
3 identity defense and credit monitoring services made necessary as mitigation measures because of
4 MGM’S Data Breach; lost benefit of their bargains and overcharges for services or products;
5 nominal and general damages; and other economic and non-economic harm.
6

7 306. By collecting and storing this PII and using it for commercial gain, MGM has a
8 duty of care to use reasonable means to secure and safeguard this PII to prevent disclosure and
9 guard against theft of the PII.

10 **SIXTH CAUSE OF ACTION**
11 **VIOLATION OF CALIFORNIA’S UNFAIR COMPETITION LAW (“UCL”)**
12 **UNLAWFUL BUSINESS PRACTICE**
13 **(Cal Bus. & Prof. Code § 17200, *et seq.*)**
14 **(By Plaintiffs Anita Johnson and Michelle Righetti,**
15 **on Behalf of the California Subclass)**

16 307. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth
17 above and incorporate them at this point by reference as though set forth in full.

18 308. Plaintiffs Johnson and Righetti bring this Count on their own behalf and on behalf
19 of the California Class (the “Class” for the purposes of this Count).

20 309. Defendant engaged in unlawful and unfair business practices in violation of Cal.
21 Bus. & Prof. Code § 17200, *et seq.* which prohibits unlawful, unfair, or fraudulent business acts
22 or practices (“UCL”).

23 310. Defendant’s conduct is unlawful because it violates the California Consumer
24 Privacy Act of 2018, Civ. Code § 1798.100, *et seq.* (the “CCPA”), and other state data security
25 laws.

26 311. Defendant stored the PII of Plaintiffs and the Class in its computer systems and
27 knew or should have known it did not employ reasonable, industry standard, and appropriate
28

1 security measures that complied with applicable regulations and that would have kept Plaintiffs’
2 and the Class’s PII secure so as to prevent the loss or misuse of that PII.

3 312. Defendant failed to disclose to Plaintiffs and the Class that their PII was not secure.
4 However, Plaintiffs and the Class were entitled to assume, and did assume that Defendant had
5 secured their PII. At no time were Plaintiffs and the Class on notice that their PII was not secure,
6 which Defendant had a duty to disclose.
7

8 313. Defendant also violated California Civil Code § 1798.150 by failing to implement
9 and maintain reasonable security procedures and practices, resulting in an unauthorized access and
10 exfiltration, theft, or disclosure of Plaintiffs’ and the Class’s nonencrypted and nonredacted PII.

11 314. Had Defendant complied with these requirements, Plaintiffs and the Class would
12 not have suffered the damages related to the data breach.
13

14 315. Defendant’s conduct was unlawful, in that it violated the CCPA.

15 316. Defendant’s acts, omissions, and misrepresentations as alleged herein were
16 unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

17 317. Defendant’s conduct was also unfair, in that it violated a clear legislative policy in
18 favor of protecting consumers from data breaches.

19 318. Defendant’s conduct is an unfair business practice under the UCL because it was
20 immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct
21 includes employing unreasonable and inadequate data security despite its business model of
22 actively collecting PII.
23

24 319. Defendant also engaged in unfair business practices under the “tethering test.” Its
25 actions and omissions, as described above, violated fundamental public policies expressed by the
26 California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 (“The Legislature declares that . . . all
27
28

1 individuals have a right of privacy in information pertaining to them . . . The increasing use of
2 computers . . . has greatly magnified the potential risk to individual privacy that can occur from
3 the maintenance of personal information.”); Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the
4 Legislature to ensure that personal information about California residents is protected.”); Cal. Bus.
5 & Prof. Code § 22578 (“It is the intent of the Legislature that this chapter [including the Online
6 Privacy Protection Act] is a matter of statewide concern.”). Defendant’s acts and omissions thus
7 amount to a violation of the law.
8

9 320. Instead, Defendant made the PII of Plaintiffs and the Class accessible to scammers,
10 identity thieves, and other malicious actors, subjecting Plaintiffs and the Class to an impending
11 risk of identity theft. Additionally, Defendant’s conduct was unfair under the UCL because it
12 violated the policies underlying the laws set out in the prior paragraph.
13

14 321. As a result of those unlawful and unfair business practices, Plaintiffs and the Class
15 suffered an injury-in-fact and have lost money or property.

16 322. The injuries to Plaintiffs and the Class greatly outweigh any alleged countervailing
17 benefit to consumers or competition under all of the circumstances.

18 323. There were reasonably available alternatives to further Defendant’s legitimate
19 business interests, other than the misconduct alleged in this complaint.
20

21 324. Therefore, Plaintiffs and the Class are entitled to equitable relief, including
22 restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to
23 Defendant because of its unfair and improper business practices; a permanent injunction enjoining
24 Defendant’s unlawful and unfair business activities; and any other equitable relief the Court deems
25 proper.
26
27
28

1 332. Because Plaintiffs and the Class were unable to protect themselves, they suffered
2 incrementally increased damages that they would not have suffered with timelier notice.

3 333. Plaintiffs and the Class are entitled to equitable relief and damages in an amount to
4 be determined at trial.
5

6 **EIGHTH CAUSE OF ACTION**
7 **VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT**
8 **Cal. Civ. Code § 1798.150**
9 **(By Plaintiffs Anita Johnson, and Michelle Righetti,**
10 **and on Behalf of the California Subclass)**

11 334. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth
12 above and incorporate them at this point by reference as though set forth in full.

13 335. Plaintiffs Johnson and Righetti bring this Count on their behalf and on behalf of the
14 California Class (the “Class” for the purposes of this Count).

15 336. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to
16 implement and maintain reasonable security procedures and practices appropriate to the nature of
17 the information to protect the nonencrypted PII of Plaintiffs and the Class. As a direct and
18 proximate result, Plaintiffs’, and the Class’s nonencrypted and nonredacted PII was subject to
19 unauthorized access and exfiltration, theft, or disclosure.

20 337. Defendant is a business organized for the profit and financial benefit of its owners
21 according to California Civil Code § 1798.140, that collects the personal information of its
22 customers, and whose annual gross revenues exceed the threshold established by California Civil
23 Code § 1798.140(d).

24 338. Plaintiffs and Class Members seek injunctive or other equitable relief to ensure
25 Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures
26 and practices. Such relief is particularly important because Defendant continues to hold PII,
27
28

1 including Plaintiffs’ and Class Members’ PII. Plaintiffs and Class Members have an interest in
2 ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing
3 to adequately safeguard this information.

4 339. Pursuant to California Civil Code § 1798.150(b), Plaintiffs mailed a CCPA notice
5 letter to Defendant’s registered service agents, detailing the specific provisions of the CCPA that
6 Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and
7 Plaintiffs believes such cure is not possible under these facts and circumstances—then Plaintiffs
8 intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.
9

10 340. As described herein, an actual controversy has arisen and now exists as to whether
11 Defendant implemented and maintained reasonable security procedures and practices appropriate
12 to the nature of the information so as to protect the personal information under the CCPA.
13

14 341. A judicial determination of this issue is necessary and appropriate at this time under
15 the circumstances to prevent further data breaches by Defendant.

16 **NINTH CAUSE OF ACTION**
17 **VIOLATION OF THE NEVADA CONSUMER FRAUD ACT**
18 **Nev. Rev. Stat. § 41.600**
19 **(By Plaintiffs and on Behalf of the Class)**

20 342. Plaintiffs repeat and reallege each and every fact, matter, and allegation set forth
21 above and incorporate them at this point by reference as though set forth in full.

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

23 1. An action may be brought by any person who is a victim of
24 consumer fraud.

25 2. As used in this section, “consumer fraud” means: . . . (e) A
26 deceptive trade practice as defined in NRS 598.0915 to 598.0925,
27 inclusive.

28 344. 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

1 or her business or occupation he or she knowingly: . . . 2) Fails to disclose a material fact in
2 connection with the sale or lease of goods or services.” MGM violated this provision because it
3 failed to disclose the material fact that its data security practices were deficient and that its cloud
4 server security settings were not adequate to protect consumers’ PII. MGM knew or should have
5 known that its data security practices were deficient. This is true because, among other things,
6 MGM was aware that the hotel industry was a frequent target of sophisticated cyberattacks. MGM
7 knew or should have known that its cloud server data security practices were insufficient to guard
8 against those attacks. MGM had knowledge of the facts that constituted the omission. MGM could
9 and should have made a proper disclosure when accepting hotel reservations, during the check-in
10 process, in the registration for its MGM Rewards loyalty program, in its Privacy Policy, or by any
11 other means reasonably calculated to inform consumers of its inadequate data security.
12

13
14 345. Also, Nev. Rev. Stat. § 598.0923(3) states: “A person engages in a ‘deceptive trade
15 practice’ when in the course of his or her business or occupation he or she knowingly: . . . 3)
16 Violates a state or federal statute or regulation relating to the sale or lease of . . . services.” MGM
17 violated this provision for several reasons, each of which is an independent predicate act for
18 purposes of violating § 598.0923(3).

19
20 346. *First*, MGM breached a Nevada statute requiring reasonable data security.
21 Specifically, Nev. Rev. Stat. § 603A.210(1) states: “A data collector that maintains records which
22 contain personal information of a resident of this State shall implement and maintain *reasonable*
23 *security measures* to protect those records from unauthorized access, acquisition, . . . use,
24 modification or disclosure.” (Emphasis added.) MGM is a data collector as defined under the
25 statute at Nev. Rev. Stat. § 603A.030. MGM failed to implement and maintain reasonable security
26 measures, evidenced by the fact that hackers accessed its cloud server and stole consumers’ PII.
27
28

1 MGM's violation of this statute was done knowingly for purposes of Nev. Rev. Stat. §
2 598.0923(3). MGM knew or should have known that its data security practices were deficient.
3 This is true because, among other things, MGM was aware that the hotel industry was a frequent
4 target of sophisticated cyberattacks. MGM knew or should have known that its cloud server data
5 security practices were insufficient to guard against those attacks. MGM had knowledge of the
6 facts that constituted the violation.
7

8 347. *Second*, MGM breached other state statutes as alleged herein. MGM also violated
9 Nev. Rev. Stat. § 598.0923(2) as alleged in this Count. MGM knew or should have known that it
10 violated these statutes. MGM's violation of each of these statutes serves as a separate predicate act
11 for purposes of violating Nev. Rev. Stat. § 598.0923(3).
12

13 348. *Third*, MGM violated the FTC Act, 15 U.S.C. § 45, as alleged above. MGM knew
14 or should have known that its data security practices were deficient, violated the FTC Act, and that
15 it failed to adhere to the FTC's data security guidance for businesses. This is true because, among
16 other things, MGM was aware that the hotel industry was a frequent target of sophisticated
17 cyberattacks. MGM knew or should have known that its cloud server data security practices were
18 insufficient to guard against those attacks. MGM had knowledge of the facts that constituted the
19 violation. MGM's violation of the FTC Act serves as a predicate act for violating Nev. Rev. Stat. §
20 598.0923(3).
21

22 349. MGM engaged in deceptive or unfair practices by engaging in conduct that is
23 contrary to public policy, unscrupulous, and caused injury to Class Members.

24 350. Plaintiffs and Class Members were denied a benefit conferred on them by the
25 Nevada legislature.

26 351. Nev. Rev. Stat. § 41.600(3) states that if the Plaintiffs prevail, the court "shall
27
28

1 award: (a) Any damages that the claimant has sustained; (b) Any equitable relief that the court
2 deems appropriate; and (c) the claimant's costs in the action and reasonable attorney's fees."

3 352. As a direct and proximate result of the foregoing, Plaintiffs and Class Members
4 suffered all forms of damages alleged herein. Plaintiffs' harms constitute compensable damages
5 under Nev. Rev. Stat. § 41.600(3).
6

7 353. Plaintiffs and Class Members are also entitled to all forms of injunctive relief
8 sought herein.

9 354. Plaintiffs and Class Members are also entitled to an award of their attorney's fees
10 and costs.

11 **PRAYER FOR RELIEF**

12 **WHEREFORE** Plaintiffs, Tonya Owens, Emily Kirwan, David Zussman, David Lackey,
13 Michael Pircio, David Terezo, Ronald G. Rundell, Anita Johnson, Paul Zari, Michael Manson,
14 Kyle Sloan, Michelle Righetti, Edgar Mejia, and DuJun Johnson, individually and on behalf of the
15 Class, request that the Court:
16

- 17 A. Certify this case as a class action on behalf of the Class defined above pursuant to
18 Rule 23(b)(2), appoint Plaintiffs as the Class Representatives;
19
20 B. Award declaratory, injunctive and other equitable relief as is necessary to protect
21 the interests of Plaintiffs and Class Members;
22
23 C. Award injunctive relief requiring Defendant to provide an accounting identifying
24 all members of the class and Class;
25
26 D. Enter a declaratory judgment that Defendant committed negligence and negligence
27 *per se* and that Defendant breached its implied contract with Plaintiffs and the
28 Class;

- 1 E. Award injunctive relief enjoining Defendant from engaging in future negligence,
2 negligence *per se*, and breaches of contract;
- 3 F. Award injunctive relief requiring Defendant to provide notice to all members of the
4 class that its data breach constituted negligence, negligence *per se*, and a breach of
5 its implied contracts with the Class, and that if they were harmed that they can bring
6 individual actions for common law relief for damages under negligence, negligence
7 *per se*, and breach of implied contract claims; and
- 8 G. Award such other and further relief as equity and justice may require.

9
10 **DEMAND FOR JURY TRIAL**

11 Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

12 Dated: January 30, 2025

13 Respectfully submitted,

14 /s/ Nathan R. Ring

15 Nathan R. Ring
16 Nevada State Bar No. 12078
17 **STRANCH, JENNINGS & GARVEY, PLLC**
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
(725) 235-9750
lasvegas@stranchlaw.com

18 *Liaison Counsel*

19 J. Gerard Stranch, IV
20 **STRANCH, JENNINGS & GARVEY, PLLC**
The Freedom Center
21 223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
22 (615) 254-8801
gstranch@stranchlaw.com

23 Lynn A. Toops
24 **COHEN & MALAD, LLP**
One Indiana Square, Suite 1400
25 Indianapolis, IN 46204
(317) 636-6481
ltoops@cohenandmalad.com

26
27 James J. Pizzirusso
HAUSFELD LLP

1 888 16th Street, Suite 300
2 Washington, DC 20006
3 (202) 540-7200
4 jpizzirusso@hausfeld.com

Interim Lead Counsel

5 Mariya Weekes
6 **MILBERG COLEMAN BRYSON PHILLIPS**
7 **GROSSMAN, PLLC**
8 201 Sevilla Avenue, 2nd Floor
9 Coral Gables, FL 33134
10 (786) 879-8200
11 mweekes@milberg.com

12 Jeff Ostrow
13 **KOPELOWITZ OSTROW, P.A.**
14 One West Las Olas Boulevard, Suite 500
15 Fort Lauderdale, FL 33301
16 (954) 525-4100
17 ostrow@kolawyers.com

18 Marc Dann
19 **DANNLAW**
20 15000 Madison Avenue
21 Lakewood, OH 44107
22 (216) 373-0539
23 mdann@dannlaw.com

24 Rachele R. Byrd
25 **WOLF HALDENSTEIN ADLER FREEMAN**
26 **& HERZ LLP**
27 750 B Street, Suite 1820
28 San Diego, CA 92101
(619) 239-4599
byrd@whafh.com

Tom Loeser
COTCHETT, PITRE & MCCARTHY
840 Malcolm Road
Burlingame, CA 94010
650-697-6000
tloeser@cpmlegal.com

Maureen M. Brady
MCSHANE & BRADY, LCC
1656 Washington Street, Suite 120
Kansas City, MO 64108
(816) 888-8010
mbrady@mcsbanebradylaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN
510 Walnut Street, Suite 500

1 Philadelphia, PA 19106
2 (215) 592-4663
cschaffer@lfsblaw.com

3 James E. Cecchi
4 **CARELLA BYRNE CECCHI OLSTEIN BRODY &**
5 **AGNELLO**
6 5 Becker Farm Road, 2nd Floor
Roseland, NJ 07068
973-994-1700
jcecchi@carellabyrne.com

7 *Plaintiffs' Steering Committee*

8 *Counsel for Plaintiffs and the Proposed Class*

9
10 **CERTIFICATE OF SERVICE**

11 It is hereby certified that a true and accurate copy of the foregoing was this 30th day of
12 January 2025 filed via the CM/ECF system and served by electronic mail upon all counsel of
13 record.

14 /s/ Nathan R. Ring
15 Nathan R. Ring
16
17
18
19
20
21
22
23
24
25
26
27
28