

1 Don Springmeyer (NBN 1021)  
KEMP JONES, LLP  
2 3800 Howard Hughes Parkway, 17th Floor  
Las Vegas, NV 89169  
3 Tel: (702) 385-6000  
4 Email: d.springmeyer@kempjones.com

5 Miles N. Clark (NBN 13848)  
KNEPPER & CLARK LLC  
6 5510 S. Fort Apache Rd., Suite 30  
Las Vegas, NV 89148-7700  
7 Tel: (702) 856-7430  
8 Email: miles.clark@knepperclark.com

9 *Co-Liaison Counsel for Plaintiffs and the Class*

10 *(Additional Counsel Listed on Signature Page)*

11  
12 **UNITED STATES DISTRICT COURT**  
**DISTRICT OF NEVADA**

13  
14 *In re: MGM Resorts International Data Breach*  
15 *Litigation*

Master Case No.: 2:20-cv-00376-GMN-NJK

**CONSOLIDATED CLASS ACTION**  
**COMPLAINT**

16 This Document Relates To: All Actions  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**TABLE OF CONTENTS**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

I. INTRODUCTION .....1

II. PARTIES.....3

    A. Plaintiffs .....3

        1. California Plaintiffs.....3

        2. Connecticut Plaintiff.....7

        3. Georgia Plaintiff.....7

        4. Louisiana Plaintiff.....8

        5. New York Plaintiff.....9

        6. Ohio Plaintiff .....9

        7. Oregon Plaintiff .....10

        8. South Carolina Plaintiff .....11

    B. Defendant .....11

III. JURISDICTION AND VENUE .....12

IV. STATEMENT OF FACTS .....13

    A. The MGM Data Breach.....13

    B. The Stolen PII Has Been Offered for Sale on the Dark Web  
        on at Least Three Occasions .....19

    C. Criminals Will Continue to Use The Stolen PII for Years.....21

    D. PII Stolen in the Data Breach Can be Combined with Data  
        Acquired Elsewhere to Commit Identity Theft.....23

    E. MGM Failed to Comply with Established Cybersecurity  
        Frameworks and Industry Standards.....25

    F. The Hotel Industry is a Frequent Target of Cyber Criminals, and  
        MGM Was on Notice of the Threat .....27

1 G. MGM Uses Consumers’ PII for Profit-Generating Purposes  
 2 Beyond Processing Hotel Stays .....29  
 3 H. Plaintiffs and Class Members Suffered Damages.....31  
 4 1. Loss of Value of PII.....32  
 5 2. Benefit of Bargain Damages.....34  
 6 I. Plaintiffs and Class Members are Entitled to Injunctive Relief .....36  
 7 V. CLASS ACTION ALLEGATIONS .....37  
 8 VI. CAUSES OF ACTION.....41  
 9 COUNT I: NEGLIGENCE .....41  
 10 COUNT II: NEGLIGENT MISREPRESENTATION .....44  
 11 COUNT III: BREACH OF IMPLIED CONTRACT.....46  
 12 COUNT IV: UNJUST ENRICHMENT .....47  
 13 COUNT V: VIOLATION OF THE NEVADA CONSUMER FRAUD  
 14 ACT, Nev. Rev. Stat. § 41.600 .....49  
 15 COUNT VI: VIOLATION OF THE CALIFORNIA UNFAIR  
 16 COMPETITION LAW (UCL), Cal. Bus. & Prof. Code §§ 17200, *et seq.* .....51  
 17 COUNT VII: VIOLATION OF THE CALIFORNIA CONSUMERS  
 18 LEGAL REMEDIES ACT (CLRA), Cal. Civ. Code §§ 1750, *et seq.* .....55  
 19 COUNT VIII: VIOLATION OF THE CALIFORNIA CUSTOMER  
 20 RECORDS ACT (CCRA), Cal. Civ. Code §§ 1798.80, *et seq.*.....59  
 21 COUNT IX: VIOLATION OF THE CONNECTICUT UNFAIR  
 22 TRADE PRACTICES ACT, Conn. Gen. Stat. § 42-110a, *et seq.*.....61  
 23 COUNT X: VIOLATION OF THE GEORGIA DECEPTIVE  
 24 TRADE PRACTICES ACT, Ga. Code Ann. §§ 10-1-370, *et seq.*.....63  
 25 COUNT XI: VIOLATION OF NEW YORK GENERAL BUSINESS  
 26 LAW, N.Y. Gen. Bus. Law § 349.....65  
 27 COUNT XII: VIOLATION OF THE OHIO DECEPTIVE TRADE  
 28 PRACTICES ACT, Ohio Rev. Code §§ 4165.01, *et seq.*.....68

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

COUNT XIII: VIOLATION OF THE OREGON UNLAWFUL  
TRADE PRACTICES ACT, Ore. Stat. §§ 646.605, *et seq.* .....70

COUNT XIV: VIOLATION OF THE OREGON CONSUMER  
INFORMATION PROTECTION ACT, Ore. Stat. §§ 646A.600, *et seq.* .....74

VII. REQUEST FOR RELIEF.....75

VIII. DEMAND FOR JURY TRIAL.....76

1 Plaintiffs Ryan Bohlim, John Dvorak, Michael Fossett, Duke Hwynn, Larry Lawter, Julie  
2 Mutsko, Andrew Sedaghatpour, Kerri Shapiro, Gennady Simkin, Robert Taylor, and Victor  
3 Wukovits (collectively “Plaintiffs”), on behalf of themselves and all others similarly situated,  
4 allege the following against Defendant MGM Resorts International (“MGM” or “Defendant”).

5 **I. INTRODUCTION**

6 1. This is a data breach class action brought on behalf of consumers whose sensitive  
7 personal information was stolen by cybercriminals in a massive cyber-attack at MGM on or around  
8 July 7, 2019 (the “Data Breach”). The Data Breach reportedly involved at least 142 million  
9 consumers, and perhaps as many as 200 million.

10 2. Information stolen in the Data Breach included names, addresses, phone numbers,  
11 email addresses, and dates of birth for guests who stayed at various hotels in the MGM corporate  
12 family. For certain guests, the stolen information also included driver’s license numbers, passport  
13 numbers, or military identification numbers (collectively “PII”).

14 3. PII stolen in the Data Breach has been posted to the “dark web” on at least three  
15 separate occasions, and continues to be extensively redistributed. MGM has acknowledged that  
16 the hacker “posted the data on a closed internet forum with the intent to sell the information for  
17 financial gain.”<sup>1</sup>

18 4. As a result of the Data Breach, Plaintiffs have experienced various types of misuse  
19 of their PII, including a fraudulent credit card account being opened in a Plaintiff’s name, a  
20 fraudulent \$800 payment from a bank account, attempted access to a bank account, fraudulent  
21 applications for cell phone service, a ransomware attack on a personal computer, fraudulent access  
22 to an online merchant account, fraudulent purchases on an Amazon account, fraudulent credit card  
23 purchases on cards previously used by Plaintiffs for their MGM hotel stays, and widespread  
24 increases in the receipt of spam emails and phone calls at email addresses and phone numbers used

---

25  
26 <sup>1</sup> See Ltr. from MGM to North Dakota Office of the Attorney General, Sept. 7, 2019, *available at*  
27 [https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2019-09-09-MGMResorts](https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2019-09-09-MGMResorts.pdf)  
28 [.pdf](https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2019-09-09-MGMResorts.pdf) (last visited Feb. 26, 2021).

1 for Plaintiffs' MGM stays. Plaintiffs have also incurred out of pocket costs, including \$2,100 for  
2 a new computer due to the ransomware incident, \$18.65 to mail a request for a credit report to  
3 Equifax, renewal costs for identity protection services, and lost wages from unpaid time off of  
4 work.

5         5. Plaintiffs and Class members have been damaged in several other ways as well. All  
6 Plaintiffs and Class members have been exposed to an increased risk of fraud, identity theft, and  
7 other misuse of their PII. Plaintiffs and Class members must now and indefinitely closely monitor  
8 their financial and other accounts to guard against fraud. This is a burdensome and time-consuming  
9 process, which was expressly recommended by MGM in light of the risk of fraud from the Data  
10 Breach. Certain Plaintiffs and Class members have also obtained copies of their credit reports and  
11 placed credit freezes and fraud alerts on their credit reports (additional burdensome steps  
12 recommended by MGM), and spent time investigating and disputing fraudulent or suspicious  
13 activity on their accounts. Plaintiffs and Class members have also suffered "benefit of the bargain"  
14 damages because they paid money to MGM for services that were intended to be accompanied by  
15 adequate data security, but were not. They also suffered a "loss of value of PII" resulting from the  
16 Data Breach.

17         6. PII stolen in the Data Breach can be misused on its own, or can be combined with  
18 personal information from other sources such as publicly available information, social media, etc.  
19 to create a package of information capable of being used to commit identity theft. Thieves can also  
20 use PII stolen in the Data Breach to send spear-phishing emails to Class members to trick them  
21 into revealing sensitive information such as login credentials, financial account numbers, Social  
22 Security numbers, and the like. Thieves can also send emails embedded with ransomware, which  
23 happened here with Plaintiff Hwynn.

24         7. The Data Breach was a direct result of MGM's failure to implement reasonable  
25 data security measures to protect Class members' PII. MGM failed to maintain and monitor its  
26 cloud-based server to protect against unauthorized intrusions. MGM also retained Class members'  
27 PII for much longer than was necessary to process Class members' hotel stays. MGM's retention  
28

1 of PII led to a massive buildup of personal information from years of transactions, left unsecured  
2 for hackers to steal.

3 8. In connection with their hotel reservations and stays, Plaintiffs were required to and  
4 did provide their PII to MGM. Plaintiffs had a reasonable expectation and understanding that  
5 MGM would adopt reasonable data security safeguards to protect their PII. MGM failed to do so,  
6 leading to the Data Breach.

7 9. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly  
8 situated consumers whose PII was stolen in the Data Breach. Plaintiffs seek remedies including:  
9 (i) compensation for the theft and misuse of their data; (ii) reimbursement of out of pocket costs;  
10 (iii) compensation for time spent responding to the Data Breach; (iv) comprehensive identity  
11 protection services paid for by MGM; and (v) injunctive relief requiring substantial improvements  
12 to MGM's data security practices, as detailed below.

13 **II. PARTIES**

14 **A. Plaintiffs**

15 **1. California Plaintiffs**

16 10. Plaintiff Ryan Bohlim is a resident of California. He paid for several hotel rooms  
17 at MGM properties prior to the Data Breach, including but not limited to at Mirage on July 8,  
18 2010, Aria on July 8, 2011, Mandalay Bay on July 11, 2011, Mirage on July 13, 2011, Luxor on  
19 July 25, 2011, MGM Grand on July 26, 2011, Mandalay Bay on July 14, 2012, Mirage on July  
20 17, 2012, Mirage on November 1, 2012, Mandalay Bay on August 4, 2013, Mandalay Bay on  
21 October 16, 2013, Mandalay Bay on February 2, 2014, Mirage on June 22, 2014, Mandalay Bay  
22 on February 1, 2015, Mirage on March 15, 2015, Mandalay Bay on November 15, 2015, Luxor  
23 on November 18, 2015, Mirage on March 22, 2016, Mirage on June 18, 2016, Mandalay Bay on  
24 February 11, 2017, Mirage on April 16, 2017, Mirage on July 14, 2017, Mirage on March 29,  
25 2018, Mirage on May 24, 2018, Excalibur on December 25, 2018, and Mandalay Bay on  
26 February 12, 2019. He booked the vast majority of his rooms by making phone calls directly to  
27 the hotels. In 2019, he received a data breach notice from MGM informing him that he was  
28

1 included in the Data Breach. He also received an alert from Credit Karma stating that his email  
2 address was found on the dark web in July 2020. That date coincides with the date on which  
3 hackers posted a batch of stolen PII from MGM on the dark web. The email address found on the  
4 dark web was the same email address he used for his MGM stays. Criminals are already using  
5 the information obtained in the Data Breach to target Plaintiff Bohlim. After the Data Breach, he  
6 experienced an increase in spam and phishing phone calls and emails at the same phone number  
7 and email address he used for his MGM stays. In response to learning of the Data Breach, he  
8 obtained a copy of his credit report to review it for fraud, and he changed several of his  
9 passwords. He has also spent time monitoring his financial and other accounts more closely than  
10 he otherwise would have. Plaintiff Bohlim values the importance of data security and the privacy  
11 of his PII. Had he known that MGM's data security practices were significantly flawed, he  
12 would not have stayed at MGM properties or would have paid less than he did for his rooms.

13 11. Plaintiff Duke Hwynn is a resident of California. He paid for several hotel rooms  
14 at MGM properties prior to the Data Breach, including at New York-New York on June 18, 2015,  
15 Aria on January 17, 2016, New York-New York on December 16, 2016, Aria on February 24,  
16 2017, New York-New York on December 23, 2018, and on various other dates at MGM Grand,  
17 Excalibur, Luxor, and Mandalay Bay. He generally booked his rooms by making phone calls  
18 directly to the hotels. Criminals are already using the information obtained in the Data Breach to  
19 target Plaintiff Hwynn. After the Data Breach, he experienced an increase in spam and phishing  
20 phone calls and emails at the same phone number and email address he used for his MGM stays.  
21 In November 2020, criminals perpetrated a ransomware attack on Plaintiff Hwynn's personal  
22 computer. He believes the ransomware was downloaded onto his computer after he opened an  
23 unfamiliar email, which was sent to the same email address he used for his MGM stays.<sup>2</sup> The

24 \_\_\_\_\_  
25 <sup>2</sup> The Identity Theft Resource Center has noted that email addresses stolen in the MGM Data  
26 Breach can be targets of emails embedded with ransomware. *See Information from MGM Data*  
27 *Breach Ends Up on the Dark Web*, Identity Theft Resource Center, July 14, 2020, available at  
<https://www.idtheftcenter.org/information-from-mgm-data-breach-ends-up-on-the-dark-web/>  
28 ("In order to get the recipient to click the link, the email just has to look like it came from MGM



1 ransomware rendered his computer inoperable, and he had to purchase a new computer, which  
2 cost approximately \$2,100. Plaintiff Hwynn had not experienced similar issues prior to the Data  
3 Breach. He spent a significant amount of time as a result of the Data Breach and its aftermath,  
4 including signing up for credit freezes with multiple credit reporting agencies, resetting various  
5 passwords, monitoring his financial and other accounts more closely than he otherwise would  
6 have, and backing up his computer multiple times as a precaution. He also had to take unpaid time  
7 off from work due to the efforts he devoted to these collective issues. He estimates that he lost  
8 several hundred dollars in aggregate unpaid wages. Plaintiff Hwynn values the importance of data  
9 security and the privacy of his PII. Had he known that MGM's data security practices were  
10 significantly flawed, he would not have stayed at MGM properties or would have paid less than  
11 he did for his rooms.

12 12. Plaintiff Andrew Sedaghatpour is a resident of California. He paid for several hotel  
13 rooms at MGM properties prior to the Data Breach, including but not limited to at Aria on May  
14 15, 2015, Aria on July 2, 2015, Aria on August 16, 2015, MGM Grand on September 3, 2015,  
15 MGM Grand on November 1, 2015, MGM Grand on May 12, 2016, Aria on May 13, 2016, Aria  
16 on December 22, 2017, and Aria on December 22, 2018. He generally booked his hotel rooms by  
17 making phone calls directly to the hotels. After the Data Breach, his H&R Block identity  
18 monitoring service notified him numerous times that his personal information including his name,  
19 email address, and phone number were found on the dark web. Criminals are already using the  
20 information obtained in the Data Breach to target Plaintiff Sedaghatpour. After the Data Breach,  
21 he experienced an increase in spam and phishing phone calls, text messages, and emails at the  
22 same phone number and email address he used for his MGM stays. Also, after the Data Breach he  
23 received many alerts stating that login attempts were made on several of his accounts from  
24 electronic devices that were not his. Plaintiff Sedaghatpour subscribed to his H&R Block identity

25 \_\_\_\_\_  
26 Resorts – or another company the person does business with – and offer some plausible reason  
27 why the recipient should open the file. From there, the malicious software, virus or even  
ransomware can be installed on the victim's computer.”) (last visited Feb. 26, 2021).

1 monitoring service prior to the Data Breach, and cannot risk cancelling the service now that his  
2 information has been compromised in the Data Breach. He has therefore renewed the service due  
3 to the Data Breach, at a cost of approximately \$26 per year. In further response to the Data Breach  
4 and its aftermath, Plaintiff Sedaghatpour has spent time monitoring his financial and other  
5 accounts more closely than he otherwise would have and resetting many of his passwords. He  
6 estimates that he spent twenty to thirty hours on these collective issues. Plaintiff Sedaghatpour  
7 values the importance of data security and the privacy of his PII. Had he known that MGM's data  
8 security practices were significantly flawed, he would not have stayed at MGM properties or would  
9 have paid less than he did for his rooms.

10 13. Plaintiff Gennady Simkin is a resident of California. He paid for several hotel  
11 rooms at MGM properties prior to the Data Breach, including at Mirage on August 31, 2012, MGM  
12 Grand on March 5, 2015, MGM Grand on March 3, 2016, Mandalay Bay on June 17, 2016, Delano  
13 on September 16, 2016, MGM Grand on November 18, 2016, New York-New York on February  
14 4, 2017, Mirage on March 17, 2017, Mirage on July 20, 2017, MGM Grand on September 21,  
15 2017, Mirage on September 28, 2017, Delano on November 2, 2017, Bellagio on December 22,  
16 2017, Mirage on September 21, 2018, and Mirage on November 1, 2018. He booked the vast  
17 majority of his rooms through the use of in-person casino hosts. Criminals are already using the  
18 information obtained in the Data Breach to target Plaintiff Simkin. After the Data Breach, he  
19 experienced various types of actual and attempted fraud. On or around June 30, 2020, criminals  
20 tried to fraudulently charge approximately \$70 on a credit card that he previously used for one or  
21 more of his MGM stays. On July 27, 2020 and July 28, 2020, criminals used his PII to impersonate  
22 him and fraudulently apply for telephone service accounts with T-Mobile and Sprint. On August  
23 16, 2020 and August 17, 2020, criminals gained access to his Amazon account and made fraudulent  
24 purchases for \$14.14 and \$21.76, which were later reversed by Amazon. These incidents were  
25 highly unusual for Plaintiff Simkin as he had not experienced any similar issues prior to the MGM  
26 Data Breach. After the Data Breach, he also experienced an increase in spam and phishing phone  
27 calls at the same phone number he used for his MGM stays. He spent a significant amount of time  
28

1 in response to the Data Breach and its aftermath, including to respond to the fraudulent items, reset  
2 various passwords, and monitor his financial and other accounts more closely than he otherwise  
3 would have. Plaintiff Simkin values the importance of data security and the privacy of his PII. Had  
4 he known that MGM's data security practices were significantly flawed, he would not have stayed  
5 at MGM properties or would have paid less than he did for his rooms.

6 **2. Connecticut Plaintiff**

7 14. Plaintiff Robert Taylor is a resident of Connecticut. He paid for several hotel rooms  
8 at MGM properties prior to the Data Breach, including at Signature MGM Grand on December  
9 17, 2014, March 2, 2015, and April 5, 2016. He booked his rooms through Expedia and Priceline.  
10 In 2019, he received a notice from MGM informing him that his PII was involved in the Data  
11 Breach. Criminals are already using the information obtained in the Data Breach to target Plaintiff  
12 Taylor. After the Data Breach, on November 18, 2019, a credit card was fraudulently opened in  
13 his name. Also, on February 23, 2021, a fraudulent \$800.00 charge was incurred on his bank  
14 account, described as a charge from a "Cash App." His bank is unwilling to reverse the charge,  
15 and he is left with the out of pocket loss. Also, after the Data Breach he noticed several inquiries  
16 on his credit reports from unfamiliar entities. After the Data Breach he also experienced an increase  
17 in spam and phishing phone calls and emails at the same phone number and email address he used  
18 for his MGM stays. He spent a significant amount of time in response to the Data Breach and its  
19 aftermath, including to investigate the fraudulent and suspicious items, reset various passwords,  
20 and monitor his financial and other accounts more closely than he otherwise would have. Plaintiff  
21 Taylor values the importance of data security and the privacy of his PII. Had he known that MGM's  
22 data security practices were significantly flawed, he would not have stayed at MGM properties or  
23 would have paid less than he did for his rooms.

24 **3. Georgia Plaintiff**

25 15. Plaintiff Michael Fossett is a resident of Georgia. He paid for several hotel rooms  
26 at MGM properties prior to the Data Breach, including but not limited to at MGM Grand, Aria,  
27 Bellagio, Mandalay Bay, Mirage, New York-New York, and MGM's Beau Rivage hotel in Biloxi,  
28

1 Mississippi. He generally booked his rooms by making phone calls directly to the hotels. After the  
2 Data Breach, he received an alert from his Credit Karma identity monitoring service linking his  
3 email address to the MGM Data Breach and stating that additional PII of his may have been  
4 involved in the breach. After the Data Breach, he also received multiple alerts from his CreditWise  
5 identity monitoring service stating that his email address has been found on the dark web. It was  
6 the same email address he used for his MGM stays. Criminals are already using the information  
7 obtained in the Data Breach to target Plaintiff Fossett. After the Data Breach, he experienced an  
8 increase in spam and phishing phone calls and emails at the same phone number and email address  
9 he used for his MGM stays. In response to the Data Breach and its aftermath, he spent a significant  
10 amount of time resetting passwords on many of his accounts. Plaintiff Fossett values the  
11 importance of data security and the privacy of his PII. Had he known that MGM's data security  
12 practices were significantly flawed, he would not have stayed at MGM properties or would have  
13 paid less than he did for his rooms.

14 **4. Louisiana Plaintiff**

15 16. Plaintiff Victor Wukovits is a resident of Louisiana. He paid for one or more hotel  
16 rooms at MGM properties prior to the Data Breach, including but not limited to at Luxor on  
17 February 4, 2017. He booked his hotel room through Hotelrates.com. Criminals are already using  
18 the information obtained in the Data Breach to target Plaintiff Wukovits. After the Data Breach,  
19 he experienced an increase in spam and phishing phone calls and emails at the same phone number  
20 and email address he used for his MGM stays. Prior to learning of the Data Breach, Plaintiff  
21 Wukovits began paying for identity monitoring and related services through Parassure at a cost of  
22 \$99 per month, and through IDAgent at a cost of \$300 per month. He cannot risk cancelling these  
23 services now that his information has been compromised by the Data Breach, and he has therefore  
24 renewed these subscriptions after learning of the Data Breach. In response to the Data Breach, he  
25 has spent time monitoring his financial and other accounts more closely than he otherwise would  
26 have. Plaintiff Wukovits values the importance of data security and the privacy of his PII. Had he  
27 known that MGM's data security practices were significantly flawed, he would not have stayed at  
28

1 an MGM property or would have paid less than he did for his room.

2 **5. New York Plaintiff**

3 17. Plaintiff Kerri Shapiro is a resident of New York. She paid for multiple hotel rooms  
4 at MGM properties prior to the Data Breach, including but not limited to at Bellagio on July 10,  
5 2016 and Aria on July 7, 2017. She booked her Bellagio room through third party Hyatt, and  
6 booked her Aria room through American Airlines Vacations. Criminals are already using the  
7 information obtained in the Data Breach to target Plaintiff Shapiro. After the Data Breach, she  
8 experienced an increase in spam and phishing phone calls and emails at the same phone number  
9 and email address she used for her MGM stays. Also, on February 28, 2021, she received a  
10 suspicious text message from AirBNB containing an unsolicited “verification code” to access her  
11 account. Her AirBNB account is linked to the same email address she used for her MGM stays.  
12 On March 22, 2021, she received an alert from Yahoo stating that a login attempt was made to her  
13 account from an unrecognized device. Her Yahoo account is linked to the Yahoo email address  
14 she used for her MGM stays. On that same day, March 22, 2021, she experienced fraudulent  
15 charges of \$41.62 and \$39.88 on her DoorDash account, which is linked to the same email address  
16 she used for her MGM stays. The DoorDash charges were reversed through her efforts. On March  
17 27, 2021, she received an email from eBay stating that her account was locked “due to concerns  
18 that someone may have used it without your permission.” Her eBay account is linked to the same  
19 email address she used for her MGM stays. In response to the Data Breach and its aftermath,  
20 Plaintiff Shapiro has spent time monitoring her financial and other accounts more closely than she  
21 otherwise would have. She also spent time obtaining and reviewing copies of her credit report on  
22 multiple occasions. Plaintiff Shapiro values the importance of data security and the privacy of her  
23 PII. Had she known that MGM’s data security practices were significantly flawed, she would not  
24 have stayed at MGM properties or would have paid less than she did for her rooms.

25 **6. Ohio Plaintiff**

26 18. Plaintiff Julie Mutsko is a resident of Ohio. She paid for multiple hotel rooms at  
27 MGM properties prior to the Data Breach, including but not limited to at Mandalay Bay on May  
28

1 20, 2014, Monte Carlo on December 7, 2014, Monte Carlo on May 18, 2015, Mandalay Bay on  
2 May 9, 2016, and MGM Grand on May 13, 2019. She generally booked her hotel rooms through  
3 third parties Vegas.com and Travelocity. Criminals are already using the information obtained in  
4 the Data Breach to target Plaintiff Mutsko. After the Data Breach, she experienced an increase in  
5 spam and phishing phone calls and emails at the same phone number and email address she used  
6 for her MGM stays. In response to the Data Breach, she spent time monitoring her financial and  
7 other accounts more closely than she otherwise would have. Plaintiff Mutsko values the  
8 importance of data security and the privacy of her PII. Had she known that MGM's data security  
9 practices were significantly flawed, she would not have stayed at MGM properties or would have  
10 paid less than she did for her rooms.

#### 11 **7. Oregon Plaintiff**

12 19. Plaintiff John Dvorak is a resident of Oregon. He paid for one or more hotel rooms  
13 at MGM properties prior to the Data Breach, including but not limited to at Excalibur on March  
14 14, 2014. He believes he booked his room through a third party service such as Expedia. After the  
15 Data Breach, Plaintiff Dvorak received an alert from his CreditWise identity monitoring service  
16 stating that his email address was found on the dark web. Criminals are already using the  
17 information obtained in the Data Breach to target Plaintiff Dvorak. He received an alert from his  
18 bank stating that someone attempted to access his "Online Banking ID" on May 25, 2020. Also,  
19 someone gained access to his account with an online merchant in May 2020 and changed the  
20 shipping name and address on the account. As a result of these issues and learning of the MGM  
21 Data Breach, he obtained a copy of his credit report from Equifax. To do so, he mailed a request  
22 to Equifax on June 1, 2020 and paid an out of pocket cost of \$18.65 to send it by registered mail,  
23 signature required. As a precaution against further fraudulent activity on his accounts, he spent  
24 time resetting several of his passwords. He also placed credit freezes on his files with key credit  
25 reporting agencies. He has also spent time monitoring his financial and other accounts more closely  
26 than he otherwise would have. He spent at least twenty hours on these collective issues. Plaintiff  
27 Dvorak values the importance of data security and the privacy of his PII. Had he known that  
28

1 MGM's data security practices were significantly flawed, he would not have stayed at MGM  
2 properties or would have paid less than he did for his room.

3 **8. South Carolina Plaintiff**

4 20. Plaintiff Larry Lawter is a resident of South Carolina. He paid for one or more hotel  
5 rooms at MGM properties prior to the Data Breach, including but not limited to at MGM Grand  
6 on May 1, 2017. He booked his room through a third-party travel agent. Criminals are already  
7 using the information obtained in the Data Breach to target Plaintiff Lawter. After the Data Breach,  
8 he experienced an increase in spam and phishing phone calls and emails at the same phone number  
9 and email address he used for his MGM stay. Plaintiff Lawter subscribed to a credit monitoring  
10 service for \$19.99 per month prior to the Data Breach, and cannot risk cancelling the service now  
11 that his information has been compromised in the Data Breach. He has therefore renewed the  
12 service after learning of the Data Breach. In response to the Data Breach, Plaintiff Lawter has spent  
13 time monitoring his financial and other accounts more closely than he otherwise would have.  
14 Plaintiff Lawter values the importance of data security and the privacy of his PII. Had he known  
15 that MGM's data security practices were significantly flawed, he would not have stayed at an  
16 MGM property or would have paid less than he did for his room.

17 **B. Defendant**

18 21. Defendant MGM Resorts International is a publicly traded company incorporated  
19 in Delaware with its headquarters at 3600 Las Vegas Boulevard South, Las Vegas, NV 89109. It  
20 is a global hospitality and entertainment company that owns, operates, and manages hotels,  
21 casinos, and resorts located predominantly in Nevada. MGM's portfolio of Nevada hotels includes  
22 MGM Grand, Aria, Bellagio, Circus Circus (sold by MGM in December 2019), Delano, Excalibur,  
23 Luxor, Mandalay Bay, The Mirage, Monte Carlo (rebranded as Park MGM in 2018), New York-  
24 New York, Signature at MGM Grand, and Vdara. MGM's portfolio of hotels outside of Nevada  
25 includes MGM Grand Detroit in Detroit, Michigan; Beau Rivage in Biloxi, Mississippi; Gold  
26 Strike Tunica in Tunica, Mississippi; Borgata in Atlantic City, New Jersey; MGM National Harbor  
27  
28

1 in Prince George’s County, Maryland; and MGM Springfield in Springfield, Massachusetts.<sup>3</sup>  
2 MGM’s consolidated revenues and net income in 2019 were \$13 billion and \$2.2 billion,  
3 respectively.

4 **III. JURISDICTION AND VENUE**

5 22. This Court has subject matter jurisdiction over this action pursuant to the Class  
6 Action Fairness Act, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds  
7 \$5,000,000 exclusive of interest and costs, there are more than 100 Class members, and at least  
8 one Class member is a citizen of a state different than Defendant.

9 23. This Court has diversity jurisdiction over Plaintiffs’ claims pursuant to 29 U.S.C. §  
10 1332(a)(1) because Plaintiffs and Defendant are citizens of different states and the amount in  
11 controversy exceeds \$75,000.

12 24. This Court has general personal jurisdiction over MGM because MGM maintains  
13 its principal place of business in this District.

14 25. This Court also has specific personal jurisdiction over MGM because MGM  
15 engaged in the conduct underlying this action in this District, including the collection, storage, and  
16 inadequate safeguarding of Plaintiffs’ PII.

17 26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a  
18 substantial part of the events giving rise to this action occurred in this District. MGM is based in  
19 this District, entered into consumer transactions with Plaintiffs in this District, and made its data  
20 security decisions leading to the Data Breach in this District.<sup>4</sup>

---

21  
22 <sup>3</sup> See MGM Resorts International Form 10-K for the year ended Dec. 31, 2019, at pg. 3, 8, 60,  
23 available at <http://d18rn0p25nwr6d.cloudfront.net/CIK-0000789570/7de59e1c-7d63-4df5-88a7-7e1ca2d0853d.pdf> (last visited Feb. 26, 2021).

24 <sup>4</sup> MGM’s key data security employees are based at MGM’s headquarters in Las Vegas. For  
25 example, MGM’s Chief Information Security Officer is based in Las Vegas. See <https://theorg.com/org/mgm-resorts-international/org-chart/branden-newman> (last visited Feb. 19, 2021). Also,  
26 a review of MGM’s information technology and data security job listings indicates that the vast  
27 majority of those positions are located in Las Vegas, including the “Vice President, Cyber  
28 Defense,” “Director of Information Security Program Management,” and “Executive Director,



1 **IV. STATEMENT OF FACTS**

2 **A. The MGM Data Breach**

3 27. On July 7, 2019, financially motivated hackers penetrated MGM’s inadequately  
4 secured networks and downloaded customer data for up to 200 million MGM guests worldwide.

5 28. MGM stated that it discovered the Data Breach three days later, on July 10, 2019.<sup>5</sup>

6 29. According to MGM, the hackers were able to obtain PII including customers’  
7 names, addresses, phone numbers, email addresses, and dates of birth. For some guests, the stolen  
8 data also included driver’s license numbers, passport numbers, or military identification numbers.<sup>6</sup>

9 30. Cybersecurity journalists have recognized that the PII stolen in the Data Breach  
10 represents a “treasure trove” of “highly sensitive” personal information, and that affected  
11 consumers now face a risk of fraud and misuse of their PII.<sup>7</sup>

12 31. On or about September 7, 2019, MGM began sending notices of the Data Breach  
13 to a limited number of the affected consumers. MGM sent a sample Notice of Data Incident  
14

15 \_\_\_\_\_  
16 Identity Access Management.” See <https://careers.mgmresorts.com/global/en/c/technology-jobs>  
(last visited Feb. 19, 2021).

17 <sup>5</sup> See *MGM Still Detangling Last Year’s Data Breach*, June 8, 2020, available at  
18 [https://www.reviewjournal.com/business/casinos-gaming/mgm-still-detangling-last-years-data-  
19 breach-2048611/](https://www.reviewjournal.com/business/casinos-gaming/mgm-still-detangling-last-years-data-breach-2048611/) (quoting MGM email sent to Canadian residents in June 2020 stating: “On July  
20 10, 2019, we learned that an unauthorized party had accessed and downloaded certain MGM  
21 Resorts guest data from an external cloud server a few days earlier.”) (last visited Feb. 26, 2021).

22 <sup>6</sup> See *MGM Resorts Says Data Breach Exposed Some Guests’ Personal Information*, The New  
23 York Times, Feb. 19, 2020, available at [https://www.nytimes.com/2020/02/19/us/mgm-data-  
24 breach.html](https://www.nytimes.com/2020/02/19/us/mgm-data-breach.html) (last visited Feb. 26, 2021); accord *MGM Admits to 2019 Data Breach Affecting 10.6  
25 Million Customers*, SC Magazine, Feb. 20, 2020, available at [https://www.scmagazine.com  
26 /home/security-news/data-breach/mgm-admits-to-2019-data-breach-affecting-10-6-million-  
27 customers/](https://www.scmagazine.com/home/security-news/data-breach/mgm-admits-to-2019-data-breach-affecting-10-6-million-customers/) (last visited Feb. 26, 2021).

28 <sup>7</sup> See *Details of 10.6 Million MGM Hotel Guests Posted on a Hacking Forum*, ZDNet, Feb. 19,  
2020, available at [https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-  
29 -guests-posted-on-a-hacking-forum/](https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/) (last visited Feb. 26, 2021); accord *MGM Resorts Hack  
30 Exposes Details of 10.6 Million Guests*, Fortune, Feb. 20, 2020, available at [https://fortune.com  
31 /2020/02/20/mgm-resorts-hack-data-breach-10-6-million-guests/](https://fortune.com/2020/02/20/mgm-resorts-hack-data-breach-10-6-million-guests/) (“Identity theft is the big threat  
32 here.”) (last visited Feb. 26, 2021).

1 (“Notice”) to the Attorneys General of various states. One such Notice stated the following:

2 **Notice of Data Incident**

3 **What Happened**

4 On or about July 7, 2019, an individual accessed MGM Resorts International’s  
5 computer network system without permission. **The individual downloaded**  
6 **partial customer data from MGM’s computer systems, then posted and**  
7 **disclosed part of the data on a closed internet forum. . . .**

8 **What Information Was Involved**

9 MGM immediately initiated an internal forensic investigation into this incident.  
10 MGM conducted an exhaustive investigation and search of the downloaded data  
11 from the closed internet site. On August 9, 2019, **MGM determined your First**  
12 **Name, Last Name and Driver’s License Number were part of the**  
13 **compromised file. . . .**

14 **What We Are Doing**

15 We take the security of our customers’ data seriously, and after MGM became  
16 aware of the event, we took immediate measures to investigate and remediate  
17 the incident. We have implemented additional safeguards to improve further  
18 data security related to external software incidents. Furthermore, MGM  
19 reported the incident to law enforcement immediately once MGM discovered  
20 the matter. In addition, we are offering identity theft protection services through  
21 ID Experts, the data incident and recovery services expert, to provide you with  
22 MyIDCare. MyIDCare services include: 12 months of credit and CyberScan  
23 monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed  
24 ID theft recovery services. With this protection, MyIDCare will help you  
25 resolve issues if your identity is compromised.

26 **What You Can Do**

27 We encourage you to contact ID Experts with any questions and to enroll in  
28 free MyIDCare services by calling 833-959-1344 or going to  
<https://ide.myidcare.com/mgmri> and using the Enrollment Code provided  
above. . . .<sup>8</sup>

32. In a similar letter to the North Dakota Attorney General dated September 7, 2019,

---

26 <sup>8</sup> See <https://media.dojmt.gov/wp-content/uploads/Consumer-Notice-26.pdf> (emphasis added)  
27 (last visited Feb. 26, 2021).

1 MGM noted that the hacker “**posted the data on a closed internet forum with the intent to sell**  
 2 **the information for financial gain.**”<sup>9</sup> The letter contained a sample Notice that was substantially  
 3 similar to the one quoted above but further specified that the Data Breach also included the theft  
 4 of “**Date[s] of Birth.**”<sup>10</sup>

5 33. MGM’s sample Notice acknowledged that consumers face a risk of fraud and  
 6 identity theft from the Data Breach. The Notice contained an attachment with several  
 7 “Recommended Steps” for consumers. Among other things, it encouraged consumers to: (i)  
 8 “Review your credit reports . . . [and] account statements” to identify any “suspicious items,” (ii)  
 9 “Place Fraud Alerts with the three credit bureaus,” and (iii) place a “Security Freeze . . . [on] your  
 10 credit files.”<sup>11</sup> It also offered consumers free credit monitoring for one year.<sup>12</sup> These steps illustrate  
 11 the very real risks faced by consumers, as well as the protective measures needed to mitigate them.  
 12 MGM would not have made these recommendations or provided free credit monitoring at its own  
 13 expense if the risk of identity theft from the Data Breach was minimal.

14 34. Aside from the sparse information provided in the Notice, MGM has kept key  
 15 details of the Data Breach private. MGM has not disclosed the size of the breach. However, on  
 16 February 19, 2020, cybersecurity journalists noted that hackers posted information of at least 10.6  
 17 million MGM hotel guests on a dark web hacking forum.<sup>13</sup> Subsequently, on July 14, 2020,  
 18

19 \_\_\_\_\_  
 20 <sup>9</sup> See [https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2019-09-09-MGM  
 Resorts.pdf](https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2019-09-09-MGMResorts.pdf) (emphasis added) (last visited Feb. 26, 2021).

21 <sup>10</sup> *Id.* (emphasis added).

22 <sup>11</sup> See <https://media.dojmt.gov/wp-content/uploads/Consumer-Notice-26.pdf> (last visited Feb. 26,  
 23 2021).

24 <sup>12</sup> *Id.*

25 <sup>13</sup> See *Details of 10.6 Million MGM Hotel Guests Posted on a Hacking Forum*, ZDNet, Feb. 19,  
 26 2020, available at [https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel  
 -guests-posted-on-a-hacking-forum/](https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/) (last visited Feb. 26, 2021); *accord MGM Admits to 2019*  
 27 *Data Breach Affecting 10.6 Million Customers*, SC Magazine, Feb. 20, 2020, available at  
 28

1 cybersecurity journalists clarified that the breach affected at least 142 million consumers, and may  
2 have affected as many as 200 million consumers:

3           The MGM Resorts 2019 data breach is much larger than initially reported, and  
4           is now believed to have impacted more than **142 million hotel guests**, and not  
5           just the 10.6 million that ZDNet initially reported back in February 2020. . . .  
6           However, the MGM data could be even bigger than the 142 million count we  
7           have today. . . . Posts on Russian-speaking hacking forums promoted the MGM  
8           data breach as containing details on more than **200 million hotel guests**.<sup>14</sup>

9           35.     MGM has not publicly disclosed the time period of the hotel stays impacted by the  
10           Data Breach. However, based on the large number of consumers affected, the stolen information  
11           presumably involved PII from hotel stays dating back years prior to the July 7, 2019 date on which  
12           the hackers stole the PII.

13           36.     MGM also has not publicly disclosed which of its hotel brands were impacted by  
14           the Data Breach. However, based on the large number of consumers involved, the stolen  
15           information presumably involved consumers who stayed at many or all of MGM’s hotel brands.

16           37.     MGM has been unusually secretive about how the hackers were able to breach its  
17           systems and obtain consumers’ PII. The scant information publicly released suggests that MGM  
18           is at fault. For example, an MGM spokesperson confirmed that the Data Breach resulted from  
19           “unauthorized access to a cloud server.”<sup>15</sup> MGM’s breach notification letters sent to Canadian  
20           residents corroborate this statement, noting that the hackers “downloaded . . . MGM Resorts guest

21 <https://www.scmagazine.com/home/security-news/data-breach/mgm-admits-to-2019-data-breach-affecting-10-6-million-customers/> (last visited Feb. 26, 2021).

22 <sup>14</sup> See *A Hacker is Selling Details of 142 Million MGM Hotel Guests on the Dark Web*, ZDNet,  
23 July 24, 2020, available at <https://www.zdnet.com/article/a-hacker-is-selling-details-of-142-million-mgm-hotel-guests-on-the-dark-web/> (emphasis added) (last visited Feb. 26, 2021).

24 <sup>15</sup> See *Details of 10.6 Million MGM Hotel Guests Posted on a Hacking Forum*, ZDNet, Feb. 19,  
25 2020, available at <https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/> (quoting unnamed “MGM spokesperson”) (last visited Feb.  
26 26, 2021).

1 data from an external cloud server.”<sup>16</sup> MGM also disclosed to the North Dakota Attorney General  
2 that the hackers “exfiltrated data by exploiting a compromised account.”<sup>17</sup>

3 38. A data security professional noted that the breach “could have easily been caused  
4 from poor cloud configuration and security hygiene.”<sup>18</sup>

5 39. Misconfigured cloud servers are a common cause of data breaches. Hackers employ  
6 automated tools that constantly scan the open internet for cloud servers with exploitable  
7 vulnerabilities. MGM knew or should have known of these risks, and should have strengthened its  
8 data security systems accordingly.

9 40. MGM also failed to encrypt the PII stored on its server, evidenced by the fact that  
10 the hackers were able to steal the PII in a readable form.

11 41. Additional details from confidential sources with insight into the Data Breach have  
12 been reported. A writer from VitalVegas.com tweeted:

13 Sources sharing juicy tidbits about the MGM Resorts data hack we haven’t seen  
14 elsewhere. Source believes hackers had ties to Iran. . . . About 52,000 people were  
15 notified, out of a reported 10.6 million.

16 Per source, data was compromised via “SQL tables” posted “in the Cloud” within  
17 AWS (Amazon Web Services). Basically, “production data” stored in a  
18 development environment.

19 \* \* \*

20 Source further explains, “due to data fields not being properly purged and tables  
21 improperly joined, those who used military I.D. and/or passport numbers had those  
22 numbers leaked along with their basic contact information.” . . . .

21 <sup>16</sup> See *MGM Still Detangling Last Year’s Data Breach*, June 8, 2020, available at [https://www.  
22 reviewjournal.com/business/casinos-gaming/mgm-still-detangling-last-years-data-breach-  
2048611/](https://www.reviewjournal.com/business/casinos-gaming/mgm-still-detangling-last-years-data-breach-2048611/) (last visited Feb. 26, 2021).

23 <sup>17</sup> See [https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2019-09-09-MGM  
24 Resorts.pdf](https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2019-09-09-MGMResorts.pdf) (last visited Feb. 26, 2021).

25 <sup>18</sup> See *MGM Admits to 2019 Data Breach Affecting 10.6 Million Customers*, SC Magazine, Feb.  
26 20, 2020, available at [https://www.scmagazine.com/home/security-news/data-breach/mgm-  
27 admits-to-2019-data-breach-affecting-10-6-million-customers/](https://www.scmagazine.com/home/security-news/data-breach/mgm-admits-to-2019-data-breach-affecting-10-6-million-customers/) (last visited Feb. 26, 2021).

1 Source says both the MGM Resorts player database (PATRON) and hotel database  
2 (OPERA) were compromised. Hackers leaked five million records to sell complete  
3 set of data, 200 million lines of data (one line of data per individual).

4 Source also claims MGM Resorts paid hackers ‘hundreds of thousands of dollars’  
5 to attempt to buy back the data, keep it from being released and to keep the data  
6 breach quiet. The data was leaked, anyway.<sup>19</sup>

7 42. The hackers stole the PII from MGM on July 7, 2019. MGM discovered the Data  
8 Breach on July 10, 2019.<sup>20</sup>

9 43. In the days and months following the Data Breach, MGM did not post any  
10 announcements of the Data Breach on its website or issue any press releases announcing the  
11 breach. Those steps are customary in large-scale data breaches like this.

12 44. MGM did not begin sending notices to affected consumers until on or around  
13 September 7, 2019, which was two months after MGM discovered the Data Breach. MGM has  
14 offered no explanation for its delay in notifying consumers. The length of the delay was  
15 unreasonable. The delay deprived Class members of the ability to take prompt steps to closely  
16 scrutinize their financial and other accounts and take other protective measures to detect and deter  
17 misuse of their data. Worse yet, MGM notified only a small fraction of the affected consumers. To  
18 this day, MGM still has not notified many – perhaps most – of the Class members.

19 45. As a result of MGM’s unreasonable delay in providing notice, and failure to notify  
20 many consumers altogether, the risk of harm to Plaintiffs and Class members has increased.

21 <sup>19</sup> See <https://twitter.com/vitalvegas/status/1231992470604402690?lang=en> (last visited Feb. 26,  
22 2021); *accord Confirmed: MGM Resorts Hack Much Bigger Than Reported*, VitalVegas.com,  
23 available at <https://vitalvegas.com/confirmed-mgm-resorts-hack-much-bigger-than-reported/>  
(last visited February 26, 2021).

24 <sup>20</sup> See *MGM Still Detangling Last Year’s Data Breach*, June 8, 2020, available at  
25 [https://www.reviewjournal.com/business/casinos-gaming/mgm-still-detangling-last-years-data-  
26 breach-2048611/](https://www.reviewjournal.com/business/casinos-gaming/mgm-still-detangling-last-years-data-breach-2048611/) (quoting MGM email sent to Canadian residents in June 2020 stating: “On July  
27 10, 2019, we learned that an unauthorized party had accessed and downloaded certain MGM  
28 Resorts guest data from an external cloud server a few days earlier.”) (last visited Feb. 26, 2021).

1 Consumer Reports has noted: “One thing that does matter is hearing about a data breach quickly.  
2 That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt  
3 them to change passwords and freeze credit reports. . . . If consumers don’t know about a breach  
4 because it wasn’t reported, they can’t take action to protect themselves.”<sup>21</sup>

5 **B. The Stolen PII Has Been Offered for Sale on the Dark Web on at Least**  
6 **Three Occasions**

7 46. The stolen PII has been posted to dark web sites used for buying and selling stolen  
8 personal information on at least three separate occasions.

9 47. MGM acknowledged that the first posting to the dark web took place on July 10,  
10 2019, three days after the hackers accessed MGM’s server.<sup>22</sup>

11 48. The initial posting was reportedly affiliated with a sophisticated hacking group  
12 known for selling stolen information:

13 According to Irina Nesterovsky, Head of Research at threat intel firm KELA, the  
14 data of [10.6 million] MGM Resorts hotel guests had been shared in some closed-  
15 circle hacking forums since at least July [2019], last year. The hacker who released  
16 this information is believed to have an association, or be a member of  
17 GnosticPlayers . . . .<sup>23</sup>

18 49. In February 2020, seven months after the initial posting to the dark web,  
19 cybercriminals were again detected posting MGM hotel guest data for sale. An article dated  
20 February 19, 2020 by data security researchers at ZDNet provided the following details:

21 **The personal details of more than 10.6 million users who stayed at MGM**  
22 **Resorts hotels have been published on a hacking forum this week.**

23 <sup>21</sup> See *The Data Breach Next Door*, Consumer Reports, Jan. 31, 2019, available at [https://www.  
24 consumerreports.org/data-theft/the-data-breach-next-door/](https://www.consumerreports.org/data-theft/the-data-breach-next-door/) (last visited Feb. 26, 2021).

25 <sup>22</sup> See [https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2019-09-09-MGM  
26 Resorts.pdf](https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2019-09-09-MGMResorts.pdf) (“On July 10, 2019, the [hacker] posted the data on a closed internet forum with the  
27 intent to sell the information for financial gain.”) (last visited Feb. 26, 2021).

28 <sup>23</sup> See *Details of 10.6 Million MGM Hotel Guests Posted on a Hacking Forum*, ZDNet, Feb. 19,  
2020, available at [https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-  
29 guests-posted-on-a-hacking-forum/](https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/) (last visited Feb. 26, 2021).

1 \* \* \*

2 ZDNet verified the authenticity of the data today, together with a security  
3 researcher from Under the Breach, a soon-to-be-launched data breach  
4 monitoring service.

5 \* \* \*

6 **According to our analysis, the MGM data dump that was shared today  
7 contains personal details for 10,683,188 former hotel guests.**

8 \* \* \*

9 Included in the leaked files are personal details such as **full names, home  
10 addresses, phone numbers, emails, and dates of birth.**

11 ZDNet reached out to past guests and confirmed they stayed at the hotel, along  
12 with their timeline, and the accuracy of the data included in the leaked files.

13 \* \* \*

14 Within an hour after we reached out to the company, we were in a conference  
15 call with the hotel chain's security team. **Within hours, the MGM Resorts  
16 team was able to verify the data and track it to a past security incident.**

17 **An MGM spokesperson told ZDNet the data that was shared online this  
18 week stems from a security incident that took place last year [in July 2019].**

19 \* \* \*

20 [T]he publication of this data dump on a very popular and openly  
21 accessibly hacking forum this week has brought it to many other hackers'  
22 attention.<sup>24</sup>

23 50. ZDNet subsequently revealed that hackers were still selling MGM customer data  
24 five months later, in July 2020. A July 14, 2020 ZDNet article stated the following:

25 [O]ver the weekend . . . a hacker put up for sale the hotel's data in an ad published on  
26 a dark web cybercrime marketplace. According to the ad, **the hacker is selling the**

27 <sup>24</sup> See *Details of 10.6 Million MGM Hotel Guests Posted on a Hacking Forum*, ZDNet, Feb. 19,  
28 2020, available at <https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/> (emphasis added) (last visited Feb. 26, 2021).



1 **details of 142,479,937 MGM hotel guests . . . .**

2 \* \* \*

3 ZDNet . . . review[ed] two different batches of MGM data -- the 10.6 million user  
4 records leaked in February and a newer 20 million batch shared by the hackers on  
5 Sunday.

6 Dates of birth and phone numbers were also included . . . .

7 \* \* \*

8 Posts on Russian-speaking hacking forums promoted the MGM data breach as  
9 containing details on more than 200 million hotel guests.<sup>25</sup>

10 51. The stolen PII has been extensively redistributed after its initial postings to the dark  
11 web. Cybersecurity experts have stated that the PII was “shared on a popular hacking forum in  
12 February 2020 where it was **extensively redistributed.**”<sup>26</sup>

13 52. These facts illustrate the significant risk of misuse faced by all Class members. The  
14 hackers stole Class members’ PII for the specific purpose of selling it to others to be misused.

15 53. Given that the data has already been posted at least three times over a twelve month  
16 period, and has been widely redistributed, there is no telling how many more times it will be re-  
17 posted or further distributed going forward.

18 **C. Criminals Will Continue to Use The Stolen PII for Years**

19 54. The risk of fraud following a data breach like this one persists for years. Identity  
20 thieves often hold stolen data for months or years before using it, to avoid detection and maximize  
21 profits. Also, the sale of stolen information on the dark web may take months or more to reach  
22 end-users, in part because data is often separated into smaller batches when sold or re-sold to  
23 appeal to different types of buyers. In addition, stolen data may be distributed through off-line

24 \_\_\_\_\_  
25 <sup>25</sup> See *A Hacker is Selling Details of 142 Million MGM Hotel Guests on the Dark Web*, ZDNet,  
26 July 24, 2020, available at <https://www.zdnet.com/article/a-hacker-is-selling-details-of-142-million-mgm-hotel-guests-on-the-dark-web/> (emphasis added) (last visited Feb. 26, 2021).

27 <sup>26</sup> See <https://haveibeenpwned.com/PwnedWebsites> (last visited Feb. 26, 2021) (emphasis added).  
28

1 criminal networks and syndicates to be used for crime near where the victim resides.

2 55. According to a Government Accountability Office Report, the threat of future  
3 identity theft lingers for a substantial period of time after a data breach due to the time lag between  
4 when information is stolen and when it is used:

5 [L]aw enforcement officials told us that in some cases, stolen data may be held  
6 for up to a year or more before being used to commit identity theft. Further,  
7 once stolen data have been sold or posted on the Web, fraudulent use of that  
8 information may continue for years. As a result, studies that attempt to measure  
the harm resulting from data breaches cannot necessarily rule out all future  
harm.<sup>27</sup>

9 56. A source specifically discussing the MGM breach stated: “[A]s with many  
10 breaches, malicious actors sometimes wait months or years to tip their hand. . . . This is a great  
11 example of how these breaches and their fallout can continue to haunt businesses for quite some  
12 time. . . . [T]he value of [this] particular dataset continues to have appeal . . . .”<sup>28</sup>

13 57. Accordingly, Class members may not see the full extent of identity theft or misuse  
14 of their personal information for years to come. They face an ongoing risk, and must vigilantly  
15 monitor their financial and other accounts indefinitely to protect against fraud.

16 58. Moreover, even after Class members’ PII is misused, it may take months or years  
17 for them to become aware of the misuse. This complicates the process of disputing and correcting  
18 the misuse of their data.

19 59. MGM’s offer of free credit monitoring for just one year is wholly inadequate in  
20 light of these long term risks.

21  
22  
23 <sup>27</sup> See *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft*  
24 *is Limited; However, the Full Extent is Unknown*, United States Government Accountability Office  
25 (June 2007), <https://www.gao.gov/assets/270/262899.pdf> (last visited Feb. 26, 2021).

26 <sup>28</sup> See *MGM Admits to 2019 Data Breach Affecting 10.6 Million Customers*, SC Magazine, Feb.  
27 20, 2020, available at [https://www.scmagazine.com/home/security-news/data-breach/mgm-](https://www.scmagazine.com/home/security-news/data-breach/mgm-admits-to-2019-data-breach-affecting-10-6-million-customers/)  
28 [admits-to-2019-data-breach-affecting-10-6-million-customers/](https://www.scmagazine.com/home/security-news/data-breach/mgm-admits-to-2019-data-breach-affecting-10-6-million-customers/) (last visited Feb. 26, 2021).

1           **D.     PII Stolen in the Data Breach Can be Combined with Data Acquired**  
2           **Elsewhere to Commit Identity Theft**

3           60.     Identity thieves can combine PII stolen in the Data Breach with information  
4 gathered elsewhere, such as from public sources or even the consumer’s social media accounts, to  
5 commit identity theft. Thieves can use the combined data to commit fraud including, among other  
6 things, opening new financial accounts or taking out loans in the consumer’s name, using the  
7 consumer’s information to obtain government benefits, filing fraudulent tax returns using the  
8 consumer’s information and retaining the resulting tax refunds, obtaining a driver’s license in the  
9 consumer’s name but with another person’s photograph, or giving false information to police  
10 during an arrest.

11           61.     A federal judge has explained this process as follows:

12                     The threat of identity theft is exacerbated by what hackers refer to as “fullz  
13 packages.” A fullz package is a dossier that compiles information about a victim  
14 from a variety of legal and illegal sources. Hackers can take information  
15 obtained in one data breach and cross-reference it against information obtained  
16 in other hacks and data breaches. So, for example, if a hacker obtains a victim’s  
17 . . . health information from UnityPoint, the hacker can combine it with the  
18 same victim’s Social Security number and phone number from a different data  
19 breach. This allows the hacker to compile a full record of information about the  
20 individual, which the hacker then sells to others as a package.

21 *Fox v. Iowa Health Sys.*, 399 F. Supp. 3d 780, 789 (W.D. Wis. 2019).

22           62.     Thieves can also use PII from the Data Breach, alone or in combination with other  
23 information about the consumer, to send highly targeted spear-phishing emails to consumers to  
24 obtain more sensitive information. Spear phishing involves sending emails that look legitimate and  
25 are accompanied by correct personal or other information about the individual. Lulled by a false  
26 sense of trust and familiarity from a seemingly valid sender (for example Bank of America,  
27 Amazon, or a government entity), the individual agrees to provide sensitive information requested  
28 in the email. This could include login credentials, account numbers, or various other types of  
information.

          63.     A journalist discussing the MGM breach pointed out that a risk of spear phishing

1 exists here, *i.e.* a “risk . . . when [the PII] is combined with other available information to forge  
2 convincing phishing or identity fraud attacks.”<sup>29</sup>

3 64. Identity thieves can also use PII from the Data Breach in a “SIM swapping” attack  
4 to take control of consumers’ phone numbers, allowing them to bypass 2-factor authentication and  
5 gain access to the consumer’s most sensitive accounts. In other words, fraudsters can use breached  
6 PII to convince the consumer’s mobile phone carrier to port the person’s mobile phone number to  
7 a phone that the hacker controls. A journalist specifically addressing the MGM breach described  
8 this scheme as follows:

9 Exposed phone numbers create an additional risk: SIM swapping. In these scams,  
10 criminals use the data they’ve gathered about a potential victim to convince  
11 wireless carriers to move a number to a different phone. The goal is to intercept  
two-factor authentication codes that are delivered by SMS.<sup>30</sup>

12 65. In light of these realities, MGM itself has acknowledged that consumers face a risk  
13 of fraud and identity theft from the Data Breach. As discussed above, MGM encouraged  
14 consumers to review their credit reports and account statements to identify suspicious activity,  
15 place fraud alerts on their credit reports with the three major credit bureaus, and place security  
16 freezes on their credit files.<sup>31</sup> MGM also offered consumers free credit monitoring for one year,  
17 which is designed to identify new accounts opened in consumers’ names. These recommendations  
18 and MGM’s offer illustrate the substantial and ongoing risks faced by all Class members.

19  
20  
21 <sup>29</sup> See *New Details Indicate That Scope of the 2019 MGM Data Breach Is Much Bigger Than*  
22 *Expected*, CPO Magazine, July 31, 2020, available at [https://www.cpomagazine.com/cyber-  
security/new-details-indicate-that-scope-of-the-2019-mgm-data-breach-is-much-bigger-than-  
expected/](https://www.cpomagazine.com/cyber-security/new-details-indicate-that-scope-of-the-2019-mgm-data-breach-is-much-bigger-than-expected/) (last visited Feb. 26, 2021).

23 <sup>30</sup> See *For Sale: Hacked Data On 142 Million MGM Hotel Guests*, Forbes, July 14, 2020,  
24 available at [https://www.forbes.com/sites/leemathews/2020/07/14/mgm-142-million-guests-  
hacked/?sh=779414ac5294](https://www.forbes.com/sites/leemathews/2020/07/14/mgm-142-million-guests-hacked/?sh=779414ac5294) (last visited Feb. 26, 2021).

25  
26 <sup>31</sup> See <https://media.dojmt.gov/wp-content/uploads/Consumer-Notice-26.pdf> (“Recommended  
27 Steps” attached to Notice) (last visited Feb. 26, 2021).  
28

1           **E.     MGM Failed to Comply with Established Cybersecurity Frameworks**  
2           **and Industry Standards**

3           66.     The Federal Trade Commission (“FTC”) has promulgated various guides for  
4 businesses, which highlight the importance of implementing reasonable data security practices.  
5 According to the FTC, the need for data security should be factored into all business decision-  
6 making.<sup>32</sup>

7           67.     In 2016, the FTC updated its publication titled *Protecting Personal Information: A*  
8 *Guide for Business*, which established cyber-security guidelines for businesses.<sup>33</sup> The guidelines  
9 stated that:

10           a)     Businesses should promptly dispose of personal identifiable information  
11 that is no longer needed, and retain sensitive data “only as long as you have a business  
12 reason to have it”;

13           b)     Businesses should encrypt sensitive personal information stored on  
14 computer networks so that it is unreadable even if hackers are able to gain access to the  
15 information;

16           c)     Businesses should thoroughly understand the types of vulnerabilities on  
17 their network and how to address those vulnerabilities;

18           d)     Businesses should install intrusion detection systems to promptly expose  
19 security breaches when they occur; and

20           e)     Businesses should install monitoring mechanisms to watch for large troves  
21 of data being transmitted from their systems.

22  
23 <sup>32</sup> See *Start With Security: A Guide for Business*, Federal Trade Commission, June 2015, available  
24 at <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business> (last  
visited Feb. 26, 2021).

25 <sup>33</sup> See *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, Oct.  
26 2016, available at [https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-](https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business)  
27 [information-guide-business](https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business) (last visited Feb. 26, 2021).  
28

1           68. In another publication, the FTC recommended that companies not maintain PII  
2 longer than is needed for authorization of a transaction; limit access to sensitive data; require  
3 complex passwords to be used on networks; use industry-tested methods for security; monitor for  
4 suspicious activity on the network; and verify that third-party service providers have implemented  
5 reasonable security measures.<sup>34</sup>

6           69. Notably, the FTC treats the failure to employ reasonable data security safeguards  
7 as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTC  
8 Act”), 15 U.S.C. § 45.

9           70. Orders from FTC enforcement actions further clarify the measures businesses must  
10 take to meet their data security obligations.

11           71. Many states’ unfair and deceptive trade practices statutes are similar to the FTC  
12 Act, and many states adopt the FTC’s interpretations of what constitutes an unfair or deceptive  
13 trade practice.

14           72. MGM’s failure to adopt reasonable safeguards to protect PII constitutes an unfair  
15 act or practice under Section 5 of the FTC Act, 15 U.S.C. § 45, and state statutory analogs.

16           73. Similarly, the U.S. Government’s National Institute of Standards and Technology  
17 (NIST) provides a comprehensive cybersecurity framework that companies of any size can use to  
18 evaluate and improve their information security controls.<sup>35</sup>

19           74. NIST publications include substantive recommendations and procedural guidance  
20 pertaining to a broad set of cybersecurity topics including risk assessments, risk management  
21 strategies, access controls, training, data security controls, network monitoring, breach detection,  
22

---

23 <sup>34</sup> See *Start With Security: A Guide for Business*, Federal Trade Commission, June 2015, available  
24 at <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business> (last  
visited Feb. 26, 2021).

25 <sup>35</sup> See *Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF  
26 STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, available at [https://nvl  
27 pubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf](https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf) (last visited Feb. 26, 2021).  
28

1 and incident response.<sup>36</sup> MGM failed to adhere to the NIST guidance.

2 75. Further, cybersecurity experts have noted various best practices that should be  
3 implemented by entities in the hotel industry, including the following:

- 4 a) Installing appropriate malware detection software;
- 5 b) Monitoring and limiting network ports;
- 6 c) Protecting web browsers and email management systems;
- 7 d) Setting up network systems such as firewalls, switches and routers;
- 8 e) Monitoring and protection of physical security systems; and
- 9 f) Training hotel staff regarding critical points.<sup>37</sup>

10 76. MGM's failure to protect massive amounts of PII illustrates its failure to adhere to  
11 the spirit and letter of the FTC guidelines, NIST guidance, and industry best practices.

12 77. MGM was well aware of its obligations to use reasonable measures to protect  
13 consumers' PII. MGM also knew it was a target for hackers, as discussed below. Despite  
14 understanding the risks and consequences of inadequate data security, MGM failed to comply with  
15 its data security obligations.

16 **F. The Hotel Industry is a Frequent Target of Cyber Criminals, and**  
17 **MGM Was on Notice of the Threat**

18 78. The type of PII collected by hotels makes this industry particularly appealing to  
19 cyber criminals.

20 79. In its 2018 Data Breach Investigations Report, Verizon noted that 15% of all data  
21 breaches occurring in 2017 involved the accommodation and food services industry.<sup>38</sup> The report

---

24 <sup>36</sup> *Id.* at Table 2 pg. 26-43.

25 <sup>37</sup> See *How to Work on Hotel Cyber Security*, Open Data Security, July 23, 2019, available at  
26 <https://opendatasecurity.io/how-to-work-on-hotel-cyber-security/> (last visited Feb. 26, 2021).

1 noted that there were 338 breaches in the accommodation industry in 2017 alone, including at  
2 many of the major hotel brands.<sup>39</sup>

3 80. Trustwave’s “2018 Global Security Report” listed hospitality as one of the top three  
4 industries targeted in payment card breaches.<sup>40</sup> Other estimates project that hotels are the targets  
5 of around 20% of all cyberattacks.<sup>41</sup>

6 81. In recent years, Choice Hotels, Hard Rock Hotel, Hilton, Hyatt, Kimpton, Marriott,  
7 Millennium, Omni, Radisson, Starwood, and Wyndham, among others, have all experienced data  
8 breach incidents.<sup>42</sup>

9 82. “Such unfortunate trends should not come as much of a surprise since hotels are  
10 hotbeds of sensitive information. Their data is spread out across porous digital systems . . . .”<sup>43</sup>

11 83. “While hospitality companies have fewer transactions than retail organizations –  
12 and thus have data on fewer customers to steal – they collect substantially more valuable and varied  
13 personal data for each of their guests. . . . This rich personal data is invaluable to cybercriminals.  
14 They can use this data to better impersonate each breached customer, leading to additional identity  
15 theft and social engineering attacks . . . . By enabling further attacks, breaching a hotel provides  
16  
17

---

18 <sup>38</sup> See *Verizon 2018 Data Breach Investigations Report*, 11th Ed., at pp. 5, 25, 27, available at  
19 [https://enterprise.verizon.com/resources/reports/DBIR\\_2018\\_Report.pdf](https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf) (last visited Feb. 26,  
20 2021).

21 <sup>39</sup> *Id.*

22 <sup>40</sup> See *Why Cybersecurity Matters*, Hotel Management, Oct. 17, 2019, available at [https://www.  
23 hotelmanagement.net/tech/why-cybersecurity-matters](https://www.hotelmanagement.net/tech/why-cybersecurity-matters) (last visited Feb. 26, 2021).

24 <sup>41</sup> *Id.*

25 <sup>42</sup> See *Timeline: The Growing Number of Hotel Data Breaches*, CoStar.com, April 7, 2020,  
26 available at <https://www.costar.com/article/139958097> (last visited Feb. 26, 2021).

27 <sup>43</sup> See *Why Cybersecurity Matters*, Hotel Management, Oct. 17, 2019, available at [https://www.  
28 hotelmanagement.net/tech/why-cybersecurity-matters](https://www.hotelmanagement.net/tech/why-cybersecurity-matters) (last visited Feb. 26, 2021).



1 cybercriminals much more value than breaching a company in almost any other industry.”<sup>44</sup>

2 84. Notably, several prior hotel data breaches involved “exposed cloud servers,” which  
3 is the same issue that reportedly led to the MGM breach.<sup>45</sup>

4 85. The high risk of data breaches in the hotel industry was widely known throughout  
5 the field, including to MGM.

6 86. Indeed, MGM acknowledged in its December 31, 2018 Form 10-K that there has  
7 been an “increase in criminal cyber security attacks against companies where customer and  
8 company information has been compromised.”<sup>46</sup> Also, MGM’s Charter for the Audit Committee  
9 of the company’s Board of Directors, dated January 17, 2019, noted that one of the Committee’s  
10 duties was to “[e]stablish and oversee procedures for . . . the Company’s plans to mitigate  
11 cybersecurity risks and respond to data breaches.”<sup>47</sup>

12 87. Thus, MGM was clearly aware of the high risk of data intrusions and the magnitude  
13 of the harm that could result from a breach. Despite the known risk, MGM failed to adopt  
14 reasonable safeguards to protect Class members’ PII.

15  
16  
17  
18  
19 <sup>44</sup> See *Cybersecurity in Hospitality: An Unsolvable Problem?*, Paladion Networks, available at  
20 <https://www.paladion.net/cybersecurity-in-hospitality-an-unsolvable-problem> (last visited Feb.  
21 26, 2021).

22 <sup>45</sup> See *MGM Admits to 2019 Data Breach Affecting 10.6 Million Customers*, SC Magazine, Feb.  
23 20, 2020, available at [https://www.scmagazine.com/home/security-news/data-breach/mgm-  
admits-to-2019-data-breach-affecting-10-6-million-customers/](https://www.scmagazine.com/home/security-news/data-breach/mgm-admits-to-2019-data-breach-affecting-10-6-million-customers/) (last visited Feb. 26, 2021).

24 <sup>46</sup> See MGM Resorts International Form 10-K for the year ended Dec. 31, 2018, at pg. 23, available  
25 at [http://d18rn0p25nwr6d.cloudfront.net/CIK-0000789570/d1b055df-9e21-4013-a311-67c98e2e  
b16a.pdf](http://d18rn0p25nwr6d.cloudfront.net/CIK-0000789570/d1b055df-9e21-4013-a311-67c98e2eb16a.pdf) (last visited Feb. 26, 2021).

26 <sup>47</sup> See [https://s22.q4cdn.com/513010314/files/doc\\_downloads/committee/MGM-Audit-  
27 Committee-Charter-\(FINAL\).pdf](https://s22.q4cdn.com/513010314/files/doc_downloads/committee/MGM-Audit-Committee-Charter-(FINAL).pdf) (last visited Feb. 26, 2021).

1 **G. MGM Uses Consumers’ PII for Profit-Generating Purposes Beyond**  
2 **Processing Hotel Stays**

3 88. Consumers’ PII is also valuable to MGM. MGM recognizes a business value of PII  
4 and collects it to better target customers and increase its profits.

5 89. MGM acknowledged that it uses consumers’ PII for the following purposes:

6 **Marketing Purposes.** We may use the information we collect for our own  
7 marketing purposes . . . .

8 **Non-Marketing Purposes.** We may use the information we collect for non-  
9 marketing purposes including . . . (2) recording and accessing gaming-  
10 related activity . . . ; (3) conducting statistical or demographic analysis; . . .  
11 (6) customizing your experience while visiting . . . MGM Resorts; (7)  
12 protecting and defending MGM Resorts International and its affiliates  
13 against legal actions or claims; . . . [and] (9) collecting debt . . . .

14 . . . . We may also link Personal Information with other generally or publicly  
15 available information to help us identify your preferences or interests. The  
16 information we collect may also be merged with information available from  
17 other sources such as (1) companies that match e-mail addresses with postal  
18 addresses and other information; . . . and (3) other subsidiaries, resorts,  
19 casinos, or properties that are owned, operated, or affiliated with MGM  
20 Resorts International.

21 \* \* \*

22 **Sharing with Business Partners and Other Third Parties.** We may share  
23 the information we collect with our business partners and other third parties  
24 for joint marketing purposes or our business partners’ (or our own)  
25 marketing purposes.<sup>48</sup>

26 90. MGM’s self-serving motive to retain and mine its customers’ PII led to MGM  
27 holding a massive trove of customer data for years after the customers’ underlying hotel stays.  
28 MGM’s data retention practices allowed the hackers to access and steal an enormous collection of  
data from years’ worth of transactions.

91. MGM retained consumers’ PII for much longer than was necessary for the business

<sup>48</sup> See <https://www.mgmresorts.com/en/privacy-policy.html>, at § 3 (last visited Feb. 15, 2021).

1 purpose for which consumers provided their PII – *i.e.*, to process their hotel stays.

2 92. The FTC has long advised against this practice, stating: “If you don’t have a  
3 legitimate business need for sensitive personally identifying information, don’t keep it. In fact,  
4 don’t even collect it. If you have a legitimate business need for the information, keep it only as  
5 long as it’s necessary.”<sup>49</sup>

6 93. As a condition of staying at its hotels, MGM required that its customers entrust it  
7 with highly sensitive PII. MGM required its customers to provide their PII during the reservation  
8 and/or check-in process. MGM retains and stores this data to make use of it for marketing purposes,  
9 among other things. By obtaining, collecting, and deriving a benefit from its customers’ PII, MGM  
10 assumed legal and equitable duties to take reasonable measures to protect their PII. MGM failed  
11 to do so, despite the known risks of theft by cyber criminals.

12 94. MGM was unjustly enriched by retaining consumers’ PII for years for its own profit  
13 motive while failing to adopt reasonable data security measures to protect that PII.

14 **H. Plaintiffs and Class Members Suffered Damages**

15 95. MGM’s failure to keep the PII of Plaintiffs and Class members secure has severe  
16 ramifications. Plaintiffs and Class members face a high risk of misuse of their PII from the Data  
17 Breach. The hackers stole PII from MGM with the specific intent to use it for illicit purposes and/or  
18 sell it to others to be misused. And the hackers have carried out this intent by posting large swaths  
19 of this data for sale at least three separate times.

20 96. Indeed, many Plaintiffs have already experienced fraudulent or suspicious use of  
21 their PII. The misuse includes a fraudulent credit card account opened in a Plaintiff’s name, a  
22 fraudulent \$800 payment from a bank account, attempted access to a bank account, fraudulent  
23 applications for cell phone service, a ransomware attack on a personal computer, fraudulent access  
24 to an online merchant account, fraudulent purchases on an Amazon account, fraudulent credit card

---

25  
26 <sup>49</sup> See *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, Oct.  
27 2016, available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business> (last visited Feb. 26, 2021).

1 purchases on cards previously used by Plaintiffs for their MGM hotel stays, and widespread  
2 increases in the receipt of spam emails and phone calls at email addresses and phone numbers used  
3 for Plaintiffs' MGM stays. These facts distinguish this case from other data breaches that involve  
4 only a speculative risk of harm.

5 97. Also, as detailed above, Plaintiffs and Class members have already incurred or will  
6 incur out of pocket costs as a result of the Data Breach.

7 98. Plaintiffs and Class members have spent and will continue to spend significant  
8 amounts of time monitoring their financial and other accounts for fraud, researching and disputing  
9 suspicious or fraudulent activity, obtaining and reviewing credit reports, placing credit freezes on  
10 their credit profiles, dealing with spam and phishing emails and phone calls, and reviewing their  
11 financial affairs more closely than they otherwise would have, among other things. These efforts  
12 are burdensome and time-consuming and would not have been necessary but for MGM's data  
13 security shortfalls.

14 99. Even in instances where a Class member is reimbursed for a financial loss due to  
15 fraud, that does not make the individual whole again because there is typically significant time and  
16 effort associated with seeking reimbursement. The Department of Justice's Bureau of Justice  
17 Statistics found that identity theft victims "reported spending an average of about 7 hours clearing  
18 up the issues" relating to fraud and identity theft.<sup>50</sup>

19 **1. Loss of Value of PII**

20 100. All Plaintiffs and Class members also suffered a "loss of value of PII."

21 101. A robust market exists for stolen PII, which is sold and distributed on the dark web  
22 and through illicit criminal networks at specific, identifiable prices. Cybercriminals routinely  
23 market stolen PII online, making the information widely available to criminals across the world.

24 102. For example, stolen driver's license numbers can be sold for between \$10 and \$35

---

25  
26 <sup>50</sup> See *Victims of Identity Theft*, U.S. Dept. of Justice, Nov. 13, 2017, available at <http://www.bjs.gov/content/pub/pdf/vit14.pdf> (last visited Feb. 26, 2021).

1 each.<sup>51</sup>

2 103. Stolen PII is a valuable commodity to identity thieves. The purpose of stealing large  
3 blocks of PII, like in the Data Breach, is to use it to for illicit purposes or to sell it and profit from  
4 other criminals who buy the data and misuse it.

5 104. That is precisely what happened here, as PII stolen in the Data Breach was posted  
6 on multiple dark web sites. The fact that PII stolen in the Data Breach was offered for sale on the  
7 dark web demonstrates that this information has a monetary value to cyber criminals.

8 105. The U.S. Attorney General stated in 2020 that consumers' sensitive personal  
9 information commonly stolen in data breaches "has economic value."<sup>52</sup> Similarly, the U.K.  
10 Information Commissioner's Office, while investigating a hotel data breach at Marriott, noted that  
11 "[p]ersonal data has a real value so organizations have a legal duty to ensure its security."<sup>53</sup>

12 106. Nevada law, too, acknowledges that personal information has intrinsic monetary  
13 value. Specifically, Nev. Rev. Stat. § 597.810 provides for statutory damages of \$750 for  
14 unauthorized commercial use of a person's name, voice, photograph, or likeness by companies  
15 conducting business in Nevada.

16 107. The value of personal information is increasingly evident in our digital economy.  
17 Many companies including MGM collect personal information for purposes of data analytics and  
18

19 \_\_\_\_\_  
20 <sup>51</sup> See <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited March 19, 2021); <https://www.keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html> (last visited March 19, 2021).

22 <sup>52</sup> See *Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military> (last visited Feb. 26, 2021).

25 <sup>53</sup> See *Intention to Fine Marriott International, Inc More Than £99 Million Under GDPR for Data Breach*, ICO News, July 9, 2019, available at <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/> (last visited Feb. 26, 2021).

1 marketing. MGM recognizes the value of personal information, collects it to better target  
2 customers to increase its profits, and shares it with third parties for similar purposes, as discussed  
3 above.

4 108. One author has noted: “Due, in part, to the use of PII in marketing decisions,  
5 commentators are conceptualizing PII as a commodity. Individual data points have concrete value,  
6 which can be traded on what is becoming a burgeoning market for PII.”<sup>54</sup>

7 109. Consumers also recognize the value of their personal information, and offer it in  
8 exchange for goods and services. The value of PII can be derived not by a price at which consumers  
9 themselves actually seek to sell it, but rather in the economic benefit consumers derive from being  
10 able to use it and control the use of it. A consumer’s ability to use their PII is encumbered when  
11 their identity or credit profile is infected by misuse or fraud. For example, a consumer with false  
12 or conflicting information on their credit report may be denied credit. Also, a consumer may be  
13 unable to open an electronic account where their email address is already associated with another  
14 user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value  
15 of the PII.

16 **2. Benefit of Bargain Damages**

17 110. Plaintiffs and Class members also suffered “benefit of bargain” damages.

18 111. Plaintiffs overpaid for hotel services that should have been – but were not –  
19 accompanied by reasonable data security.

20 112. One component of the cost of Class members’ hotel rooms was the implicit promise  
21 MGM made to Class members to protect their PII. Part of the price consumers paid to MGM was  
22 intended to be used to provide adequate data security. MGM did not do so. Thus, consumers did  
23 not get what they paid for.

24 113. Because of the value consumers place on data privacy and security, companies with  
25

---

26 <sup>54</sup> See John T. Soma, *Corporate Privacy Trend: The “Value” of Personally Identifiable*  
27 *Information (‘PII’) Equals the “Value” of Financial Assets*, 15 Rich. J. L. & Tech. 11, 14 (2009).

1 robust data security practices can command higher prices than those that do not, and vice versa.

2 114. Had Plaintiffs known the truth about MGM's deficient data security practices, they  
3 would not have stayed at MGM properties or would have paid less than they did for their rooms.

4 115. Plaintiffs and Class members did not receive the benefit of their bargain because  
5 they paid for data security safeguards they expected but did not receive.

6 116. Plaintiffs and Class members are entitled to monetary compensation for the various  
7 types of damages discussed above.

8 117. They are also entitled to payment for a robust set of identity protection services,  
9 including credit monitoring. Such services are reasonable and necessary here. The stolen PII is  
10 historical in nature and can be used for identity theft and other types of financial fraud. There is  
11 no question that the PII was taken by sophisticated cybercriminals, increasing the risks to Class  
12 members. The consequences of identity theft are serious and long-lasting. There is a benefit to  
13 early detection and monitoring. Experts recommend that data breach victims obtain identity  
14 protection services for many years after a data breach – beyond the 12-month limit that MGM  
15 offered to certain victims for a limited time under an inadequate protection plan. Annual  
16 subscriptions for comprehensive identity protection services that include three-bureau credit  
17 monitoring, alerts on credit inquiries and new account openings, fraud resolution services, dark  
18 web monitoring, and identity theft insurance range from \$219 to \$329 per year.<sup>55</sup> MGM must  
19 provide monetary compensation to Class members to pay for these services.

20 118. As a result of the Data Breach, Plaintiffs and Class members have suffered and/or  
21 will suffer or continue to suffer economic loss and other actual harm for which they are entitled to  
22 damages, including but not limited to the following:

- 23 (a) losing the inherent value of their PII;
- 24

---

25 <sup>55</sup> See Robert McMillan & Deepa Seetharaman, *Facebook Finds Hack Was Done By Spammers,*  
26 *Not Foreign State*, THE WALL STREET JOURNAL (Oct. 17, 2018), available at [https://www.wsj.com](https://www.wsj.com/articles/facebook-tentatively-concludes-recent-hack-was-perpetrated-by-spammers-1539821869)  
27 [/articles/facebook-tentatively-concludes-recent-hack-was-perpetrated-by-spammers-1539821869](https://www.wsj.com/articles/facebook-tentatively-concludes-recent-hack-was-perpetrated-by-spammers-1539821869)  
(last visited Feb. 26, 2021).

1 (b) purchasing hotel room rentals that they would not have otherwise paid for,  
2 and/or paying more for the rooms than they otherwise would have paid, had they known  
3 the truth about MGM’s substandard data security practices;

4 (c) losing the value of MGM’s implied promises of adequate data security;

5 (d) identity theft and fraud resulting from the theft of their PII;

6 (e) costs associated with the detection and prevention of identity theft and  
7 unauthorized use of their financial and other accounts;

8 (f) costs associated with purchasing credit monitoring and identity protection  
9 services;

10 (g) unauthorized charges and loss of use of and access to their financial account  
11 funds, and costs associated with the inability to obtain money from their accounts,  
12 including missed payments, late charges, and other fees;

13 (h) costs associated with time spent and the loss of productivity or the  
14 enjoyment of one’s life from taking time to address and attempt to mitigate the actual and  
15 future consequences of the Data Breach; and

16 (i) the continued imminent and certainly impending injury flowing from  
17 potential fraud and identify theft posed by their PII being in the possession of unauthorized  
18 third parties.

19 **I. Plaintiffs and Class Members are Entitled to Injunctive Relief**

20 119. MGM acted on grounds that apply generally to the Class as a whole. Thus,  
21 injunctive relief is appropriate on a class-wide basis.

22 120. Plaintiffs and Class members are entitled to injunctive relief requiring MGM to,  
23 among other things:

24 (a) Strengthen its technical and administrative information security controls  
25 and adequately fund them for several years;

26 (b) Submit to regular, independent System and Organization Controls 2 (“SOC  
27 2”) Type 2 audits of its enterprise data networks and all security-relevant systems, with  
28



1 scoping and assertion statements established by an independent assessor;

2 (c) Promptly implement all remediation measures recommended by the SOC 2,  
3 Type 2 assessor and any other forensic analysis or incident response entities retained to  
4 address the Data Breach;

5 (d) Implement tokenization or column-level encryption of sensitive PII in all  
6 databases;

7 (e) Purge all PII that MGM no longer needs for processing Class members’  
8 prior hotel stays; and

9 (f) Delete all PII from non-production database environments.

10 121. These measures are necessary to guard against future data breaches at MGM  
11 involving Class members’ PII that MGM continues to retain.

12 122. Indeed, MGM still has not addressed many publicly reported security flaws on its  
13 website. According to UpGuard, a company that publishes information security ratings, eight  
14 months after the Data Breach the MGM Resorts website was still “at risk of being hijacked,”  
15 “[v]ulnerable to cross-site scripting,” and “[s]usceptible to man-in-the-middle attacks.”<sup>56</sup> As of  
16 February 2021, the MGM Resorts website was again flagged for additional security  
17 vulnerabilities.<sup>57</sup>

18 123. If MGM cannot secure known vulnerabilities in its public-facing website, it is likely  
19 that even more serious vulnerabilities continue to exist inside its networks, where it stores Class  
20 members’ data.

21 **V. CLASS ACTION ALLEGATIONS**

22 124. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), (b)(2),  
23  
24

---

25 <sup>56</sup> See <https://www.upguard.com/security-report/mgmresorts> (last visited March 2020).  
26

27 <sup>57</sup> See <https://www.upguard.com/security-report/mgmresorts> (last visited Feb. 28, 2021).  
28

1 (b)(3), and (c)(4).

2 **NATIONWIDE CLASS**

3 125. Plaintiffs seek certification of the following class:

4 Nationwide Class: All persons residing in the United States whose PII was  
5 acquired by cybercriminals in the MGM Data Breach.

6 126. The Nationwide Class asserts claims against MGM for Negligence (Count I),  
7 Negligent Misrepresentation (Count II), Breach of Implied Contract (Count III), Unjust  
8 Enrichment (Count IV), and violation of the Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600  
9 (Count V).

10 127. Under the Restatement (Second) of Conflict of Laws §§ 145 and 188 adopted by  
11 Nevada courts and applied to the facts here, Nevada substantive law controls the common law tort  
12 and contract-based claims of all Plaintiffs, regardless of Plaintiffs' states of residency.

13 128. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600, may be applied on a  
14 nationwide basis because MGM's unlawful conduct was centered in Nevada.

15 **STATEWIDE SUBCLASSES**

16 129. In the alternative to the Nevada Consumer Fraud Act claim, certain Plaintiffs assert  
17 claims for violation of their home states' unfair or deceptive trade practices statutes.

18 130. Certain Plaintiffs also assert claims for violation of their home states' data security  
19 statutes for MGM's failure to implement adequate data security.

20 131. Plaintiffs seek certification of the following statewide subclasses ("Subclasses") for  
21 Plaintiffs' state statutory claims asserting unfair or deceptive trade practices and/or failure to  
22 implement adequate data security:

23 California Subclass: All residents of California whose PII was acquired by  
24 cybercriminals in the MGM Data Breach.

25 Connecticut Subclass: All residents of Connecticut whose PII was acquired by  
26 cybercriminals in the MGM Data Breach.

27 Georgia Subclass: All residents of Georgia whose PII was acquired by cybercriminals  
28 in the MGM Data Breach.

1            New York Subclass: All residents of New York whose PII was acquired by  
2            cybercriminals in the MGM Data Breach.

3            Ohio Subclass: All residents of Ohio whose PII was acquired by cybercriminals in the  
4            MGM Data Breach.

5            Oregon Subclass: All residents of Oregon whose PII was acquired by cybercriminals  
6            in the MGM Data Breach.

7            132.    The statewide Subclasses assert state statutory claims for violation of the California  
8            Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.* (Count VI); California  
9            Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* (Count VII); California Customer  
10           Records Act, Cal. Civ. Code §§ 1798.80, *et seq.* (Count VIII); Connecticut Unfair Trade Practices  
11           Act, Conn. Gen. Stat. § 42-110a, *et seq.* (Count IX); Georgia Deceptive Trade Practices Act, Ga.  
12           Code Ann. §§ 10-1-370, *et seq.* (Count X); New York General Business Law, N.Y. Gen. Bus. Law  
13           § 349 (Count XI); Ohio Deceptive Trade Practices Act, Ohio Rev. Code §§ 4165.01, *et seq.* (Count  
14           XII); Oregon Unlawful Trade Practices Act, Ore. Stat. §§ 646.605, *et seq.* (Count XIII); and  
15           Oregon Consumer Information Protection Act, Ore. Stat. §§ 646A.600, *et seq.* (Count XIV).

16           133.    Excluded from the Nationwide Class and all Subclasses (collectively the “Class”)  
17           are Defendant’s executive officers and directors, the judges to whom this case is assigned, their  
18           immediate family members, and courtroom staff.

19           134.    Plaintiffs reserve the right to amend the definitions of the Classes after having an  
20           opportunity to conduct discovery.

21           135.    Numerosity: Fed. R. Civ. P. 23(a)(1). The Nationwide Class and statewide  
22           Subclasses are each so numerous that joinder of all members is impracticable. While the exact  
23           number of Class members is unknown to Plaintiffs at this time, media reports indicate that the PII  
24           of up to 200 million consumers worldwide was stolen in the Data Breach. It is unclear how many  
25           of those consumers are U.S. residents and therefore Class members here. The class size can be  
26           determined by information available in MGM’s records, which will be the subject of discovery in  
27           the litigation. On information and belief, there are at least tens of millions of Class members in the  
28           Nationwide Class, and at least thousands of Class members in each statewide Subclass.

1           136. Commonality: Fed. R. Civ. P. 23(a)(2). There are many questions of “law or fact”  
2 common to the Class for purposes of Rule 23(a)(2), including but not limited to:

3           (a) Whether MGM’s data security systems prior to the Data Breach complied  
4 with applicable data security laws, regulations, industry standards, and other relevant  
5 requirements;

6           (b) Whether MGM owed a duty to Plaintiffs and Class members to safeguard  
7 their PII;

8           (c) Whether MGM breached its duty to Plaintiffs and Class members to  
9 safeguard their PII;

10           (d) Whether MGM knew or should have known that its data security systems  
11 were deficient prior to the Data Breach;

12           (e) Whether MGM had an implied contractual obligation to adopt reasonable  
13 data security measures;

14           (f) Whether MGM’s conduct constituted violations of state consumer  
15 protection statutes;

16           (g) Whether MGM’s conduct constituted violations of state data security  
17 statutes;

18           (h) Whether Plaintiffs and Class members suffered legally cognizable damages;  
19 and

20           (i) Whether Plaintiffs and Class members are entitled to injunctive relief.

21           137. Typicality: Fed. R. Civ. P. 23(a)(3). Typicality is satisfied here because the claims  
22 of Plaintiffs and all Class members are derived from the same operative facts. All Plaintiffs and  
23 Class members had their PII stolen in the Data Breach. Plaintiffs and Class members have the same  
24 basic legal claims against MGM.

25           138. Adequacy of Representation: Fed R. Civ. P. 23(a)(4). Plaintiffs will fairly and  
26 adequately protect the interests of the Class. Plaintiffs have retained competent counsel who are  
27 highly experienced in data breach class actions and other complex litigation. Plaintiffs and their  
28

1 counsel are committed to prosecuting this action vigorously on behalf of the Class. Plaintiffs’  
2 counsel have the financial and personnel resources to litigate this matter through all phases of  
3 pretrial litigation, trial, and any necessary appeals. Neither Plaintiffs nor their counsel have any  
4 interests that are contrary to, or conflict with, those of the Class.

5 139. Predominance: Fed. R. Civ. P. 23(b)(3). MGM has engaged in a common course of  
6 conduct toward all Class members. The common issues identified above predominate over any  
7 issues affecting only individual Class members. The common issues hinge upon MGM’s conduct  
8 rather than that of any individual Plaintiff or Class member. Adjudication of the common issues  
9 in a single action has important and desirable advantages that will lead to judicial economy.

10 140. Superiority: Fed. R. Civ. P. 23(b)(3). A class action is superior to other available  
11 methods for the fair and efficient adjudication of the controversy. Class treatment of common  
12 questions of law or fact is superior to multiple individual actions or piecemeal litigation. The  
13 litigation of separate actions by consumers would create a risk of inconsistent or varying  
14 adjudications, which could establish incompatible standards of conduct for MGM. In contrast,  
15 conducting this action on a class-wide basis presents fewer management difficulties, conserves  
16 judicial and party resources, and pursues the rights of all Class members in a single proceeding.  
17 Also, absent a class action, most Class members would find that the cost of litigating their  
18 individual claims is prohibitively high and they would therefore have no realistic means to a  
19 remedy on an individual non-class basis.

20 141. Injunctive Relief: Fed. R. Civ. P. 23(b)(2). MGM acted on grounds that apply  
21 generally to the Class as a whole. MGM continues to retain Class members’ PII, which is subject  
22 to future data breaches while in MGM’s possession. Injunctive relief is therefore appropriate on a  
23 class-wide basis.

24 142. Issue Classes: Fed. R. Civ. P. 23(c)(4). Under Rule 23(c)(4), an “action may be  
25 brought or maintained as a class action with respect to particular issues.” Fed. R. Civ. P. 23(c)(4).  
26 Various issues here are appropriate for class treatment because such matters present common class-  
27 wide issues, the resolution of which would advance the disposition of this action and the parties’  
28

1 interests. Such issues include, but are not limited to, those identified in the Commonality section  
2 above.

3 **VI. CAUSES OF ACTION**

4 **COUNT I**  
5 **NEGLIGENCE**  
6 **(On Behalf of the Nationwide Class)**

7 143. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully  
8 set forth herein.

9 144. As a condition of receiving MGM's services, Plaintiffs and all Class members were  
10 required to provide MGM with their PII.

11 145. Plaintiffs and Class members entrusted their PII to MGM with the understanding  
12 that MGM would take reasonable measures to safeguard their PII.

13 146. MGM had knowledge of the sensitivity of the PII and the types of harm that  
14 Plaintiffs and Class members could face if their PII was stolen in a data breach.

15 147. MGM had a duty to exercise reasonable care in safeguarding, securing, and  
16 protecting Class members' PII. This duty included, among other things, designing, maintaining,  
17 and testing MGM's data security procedures to ensure that the PII was adequately protected, that  
18 cloud-based safeguards were adequately implemented, and that employees tasked with  
19 maintaining PII were adequately trained on cybersecurity measures.

20 148. MGM's duty of care arose from, among other things:

21 (a) the special relationship that existed between MGM and its customers  
22 because MGM was in an exclusive position to ensure that its systems were sufficient to  
23 protect against the foreseeable risk that a data breach could occur;

24 (b) Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . .  
25 practices in or affecting commerce," including, as interpreted and enforced by the FTC,  
26 failing to adopt reasonable data security measures;

27 (c) general common law duties to adopt reasonable data security measures to  
28 protect customer PII and to act as a reasonable and prudent person under the same or similar

1 circumstances would act; and

2 (d) state statutes requiring reasonable data security measures, including but not  
3 limited to Nev. Rev. Stat. § 603A.210, which states that businesses possession personal  
4 information of Nevada residents “shall implement and maintain reasonable security  
5 measures to protect those records from unauthorized access.”

6 149. MGM was subject to an “independent duty,” untethered to any express contract  
7 between MGM and Class members. The sources of MGM’s independent duty are included in the  
8 list above.

9 150. MGM’s violation of the FTC Act and state data security statutes constitutes  
10 negligence *per se* for purposes of establishing the duty and breach elements of Plaintiffs’  
11 negligence claim. Those statutes were designed to protect a group to which Plaintiffs belong and  
12 to prevent the type of harm that resulted from the Data Breach.

13 151. MGM is a multi-billion-dollar publicly traded company that had the financial and  
14 personnel resources necessary to prevent the Data Breach. MGM nevertheless failed to adopt  
15 reasonable data security measures, in breach of the duties it owed to Plaintiffs and Class members.

16 152. Plaintiffs and Class members were the foreseeable victims of MGM’s inadequate  
17 data security. MGM knew that a breach of its systems could cause harm to Plaintiffs and Class  
18 members.

19 153. MGM’s conduct created a foreseeable risk of harm to Plaintiffs and Class members.  
20 MGM’s conduct included its failure to adequately restrict access to its cloud server that held  
21 consumers’ PII.

22 154. MGM knew or should have known of the inherent risks in collecting and storing  
23 massive amounts PII, the importance of providing adequate data security over that PII, and the  
24 frequent cyberattacks within the hotel industry.

25 155. Plaintiffs and Class members had no ability to protect their PII once it was in  
26 MGM’s possession and control. MGM was in an exclusive position to protect against the harm  
27 suffered by Plaintiffs and Class members as a result of the Data Breach.

28

1 156. MGM, through its actions and inactions, breached its duties owed to Plaintiffs and  
2 Class members by failing to exercise reasonable care in safeguarding their PII while it was in  
3 MGM's possession and control. MGM's breaches of duties included, among other things, its: (i)  
4 failure to adopt reasonable data security practices; (ii) failure to encrypt the PII in its systems; (iii)  
5 retention of PII for much longer than was necessary for processing consumers' hotel stays; and  
6 (iv) failure to provide adequate and timely notice of the Data Breach to consumers.

7 157. MGM inadequately safeguarded consumers' PII in deviation of standard industry  
8 rules, regulations, and best practices at the time of the Data Breach.

9 158. But for MGM's breach of duties, consumers' PII would not have been stolen.

10 159. There is a temporal and close causal connection between MGM's failure to  
11 implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiffs  
12 and Class members.

13 160. As a result of MGM's negligence, Plaintiffs and Class members suffered and will  
14 continue to suffer the various types of damages alleged herein.

15 161. Plaintiffs and Class members are entitled to all forms of monetary compensation  
16 set forth herein, including monetary payments to provide adequate identity protection services.  
17 Plaintiffs and Class members are also entitled to the injunctive relief sought herein.

18 **COUNT II**  
19 **NEGLIGENT MISREPRESENTATION**  
20 **(On Behalf of the Nationwide Class)**

21 162. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully  
22 set forth herein.

23 163. Nevada has adopted the Restatement (Second) of Torts § 551 (1977), which  
24 imposes liability for negligent misrepresentations based on omissions. Section 551, titled  
25 "Liability for Nondisclosure," states:

26 One who fails to disclose to another a fact that he knows may justifiably induce the  
27 other to act or refrain from acting in a business transaction is subject to the same  
28 liability to the other as though he had represented the nonexistence of the matter  
that he has failed to disclose, if . . . he is under a duty to the other to exercise



1 reasonable care to disclose the matter in question.

2 164. MGM failed to disclose to Plaintiffs and Class members that it did not employ  
3 reasonable safeguards to protect consumers' PII.

4 165. MGM's omissions were made for the guidance of consumers in their transactions  
5 with MGM.

6 166. MGM failed to disclose facts that MGM knew may justifiably induce consumers to  
7 act or refrain from acting in their business transactions with MGM.

8 167. MGM's omissions were made in the course of MGM's business.

9 168. MGM had a duty to speak regarding the inadequacy of its data security practices  
10 and its inability to reasonably protect consumers' PII.

11 169. MGM knew or should have known that its data security practices were deficient.  
12 This is true because, among other things, MGM was aware that the hotel industry was a frequent  
13 target of sophisticated cyberattacks. MGM knew or should have known that its data security  
14 practices were insufficient to guard against those attacks.

15 170. MGM was in a special relationship with, or relationship of trust and confidence  
16 relative to, consumers. MGM was in an exclusive position to ensure that its safeguards were  
17 sufficient to protect against the foreseeable risk that a data breach could occur. MGM was also in  
18 exclusive possession of the knowledge that its data security processes and procedures were  
19 inadequate to safeguard consumers' PII.

20 171. MGM's omissions were material given the sensitivity of the PII maintained by  
21 MGM and the gravity of the harm that could result from theft of the PII.

22 172. Data security was an important part of the substance of the transactions between  
23 MGM and consumers.

24 173. MGM knew that consumers would enter into business transactions under a mistake  
25 as to facts basic to the transactions. Because of the relationship between the parties, consumers  
26 would reasonably expect a disclosure of the basic facts regarding MGM's inadequate data security.

27 174. Had MGM disclosed to Plaintiffs and Class members that its systems were not  
28

1 secure and thus were vulnerable to attack, Plaintiffs and Class members would not have entrusted  
2 their PII to MGM.

3 175. MGM should have made a proper disclosure to consumers when accepting hotel  
4 reservations, during the check-in process, or by any other means reasonably calculated to inform  
5 consumers of its inadequate data security.

6 176. In addition to its omissions, MGM is also liable for its implied misrepresentations.  
7 MGM required consumers to provide their PII during the reservation and/or check-in process. In  
8 doing so, MGM made implied or implicit representations that it employed reasonable data security  
9 practices to protect consumers' PII. By virtue of accepting Plaintiffs' PII during the reservation  
10 and check-in process, MGM implicitly represented that its data security processes were sufficient  
11 to reasonably safeguard the PII. This constituted a negligent misrepresentation.

12 177. MGM failed to exercise reasonable care or competence in communicating its  
13 omissions and misrepresentations.

14 178. As a direct and proximate result of MGM's omissions and misrepresentations,  
15 Plaintiffs and Class members suffered the various types of damages alleged herein.

16 179. Plaintiffs and Class members are entitled to all forms of monetary compensation  
17 and injunctive relief set forth herein.

18 **COUNT III**  
19 **BREACH OF IMPLIED CONTRACT**  
20 **(On Behalf of the Nationwide Class)**

21 180. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully  
22 set forth herein.

23 181. When Plaintiffs and Class members provided consideration and PII to MGM in  
24 exchange for MGM's services, they entered into implied contracts with MGM under which MGM  
25 agreed to adopt reasonable safeguards to protect their PII.

26 182. MGM solicited and invited Plaintiffs and Class members to purchase hotel room  
27 rentals. As part of the rental and/or reservation process, Plaintiffs and Class members were  
28 required to provide their PII as a condition of the rental or reservation.

1 183. When entering into implied contracts, Plaintiffs and Class members reasonably  
2 believed and expected that MGM would implement reasonable data security measures and that  
3 MGM's data security practices complied with relevant laws, regulations, and industry standards.  
4 MGM knew or should have known that Plaintiffs and Class members held this belief and  
5 expectation.

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

12 185. MGM's conduct in requiring consumers to provide PII as a prerequisite to their  
13 hotel stays illustrates MGM's intent to be bound by an implied promise to adopt reasonable data  
14 security measures.

15 186. Plaintiffs and Class members would not have provided their PII to MGM in the  
16 absence of MGM's implied promise to keep the PII reasonably secure.

17 187. Plaintiffs and Class members fully performed their obligations under their implied  
18 contracts with MGM. They provided consideration and their PII to MGM in exchange for MGM's  
19 services and its implied promise to adopt reasonable data security measures.

20 188. MGM breached its implied contracts with Plaintiffs and Class members by failing  
21 to implement reasonable data security measures.

22 189. As a result of MGM's conduct, Plaintiffs and Class members have suffered, and  
23 continue to suffer, legally cognizable damages set forth herein, including nominal damages.

24 190. Plaintiffs and Class members are entitled to all forms of monetary compensation  
25 and injunctive relief set forth herein.

26  
27  
28

**COUNT IV**  
**UNJUST ENRICHMENT**  
**(On Behalf of the Nationwide Class)**

1  
2  
3       191. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully  
4 set forth herein.

5       192. This claim is plead in the alternative to Plaintiffs' breach of implied contract claim.

6       193. Plaintiffs and Class members conferred benefits upon MGM.

7       194. In exchange for providing money and PII to MGM, Plaintiffs and Class members  
8 should have received hotel room rentals accompanied by adequate safeguarding of their PII.

9       195. MGM profited from its transactions with Class members in two ways. First, MGM  
10 received monetary consideration as revenue. Second, MGM used Class members' PII for a variety  
11 of profit-generating purposes beyond simply providing hotel rooms. MGM used the PII for  
12 marketing and other purposes as discussed more fully above. MGM used the PII to generate future  
13 stays from consumers and derive future revenues and profit, among other things.

14       196. The money Plaintiffs and Class members provided to MGM for hotel room rentals  
15 was intended to be used by MGM, in part, to fund reasonable data security.

16       197. MGM failed to provide reasonable data security, yet it kept all monies paid by  
17 Plaintiffs and Class members.

18       198. MGM knew that Plaintiffs and Class members conferred monetary and other  
19 benefits on MGM. MGM accepted those benefits.

20       199. MGM also retained the PII for much longer than was reasonably necessary to  
21 process consumers' hotel stays. MGM benefitted from that PII, without providing a return benefit  
22 to consumers.

23       200. Under principles of equity and good conscience, MGM should not be permitted to  
24 retain the full monetary benefit of its transactions with Plaintiffs and Class members. MGM failed  
25 to adequately secure consumers' PII and, therefore, did not provide the full services that consumers  
26 paid for.

27       201. MGM acquired consumers' money and PII through inequitable means in that it  
28

1 failed to disclose its inadequate data security practices when entering into transactions with  
2 consumers and obtaining their PII.

3 202. If Plaintiffs and Class members would have known that MGM employed  
4 inadequate data security safeguards, they would not have agreed to transact with MGM or would  
5 have transacted only at reduced prices.

6 203. Class members have no adequate remedy at law. MGM continues to retain Class  
7 members' PII while exposing the PII to a risk of future data breaches while in MGM's possession.  
8 MGM also continues to derive a financial benefit from using Class members' PII.

9 204. As a direct and proximate result of MGM's conduct, Plaintiffs and Class members  
10 have suffered the various types of damages alleged herein.

11 205. MGM should be compelled to disgorge into a common fund or constructive trust,  
12 for the benefit of Class members, the proceeds that they unjustly received from Class members. In  
13 the alternative, MGM should be compelled to refund the amounts that Class members overpaid for  
14 MGM's services.

15 **COUNT V**  
16 **VIOLATION OF THE NEVADA CONSUMER FRAUD ACT**  
17 **Nev. Rev. Stat. § 41.600**  
18 **(On Behalf of the Nationwide Class)**

19 206. Plaintiffs re-allege and incorporate by reference all preceding allegations as if fully  
20 set forth herein.

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

- 22 1. An action may be brought by any person who is a victim of  
23 consumer fraud.
- 24 2. As used in this section, "consumer fraud" means: . . . (e) A deceptive  
25 trade practice as defined in NRS 598.0915 to 598.0925, inclusive.

26 208. In turn, Nev. Rev. Stat. § 598.0923(2) (part of the Nevada Deceptive Trade  
27 Practices Act) states: "A person engages in a 'deceptive trade practice' when in the course of his  
28 or her business or occupation he or she knowingly: . . . 2) Fails to disclose a material fact in  
connection with the sale or lease of goods or services." MGM violated this provision because it

1 failed to disclose the material fact that its data security practices were inadequate to reasonably  
2 safeguard consumers' PII. MGM knew or should have known that its data security practices were  
3 deficient. This is true because, among other things, MGM was aware that the hotel industry was a  
4 frequent target of sophisticated cyberattacks. MGM knew or should have known that its data  
5 security practices were insufficient to guard against those attacks. MGM had knowledge of the  
6 facts that constituted the omission. MGM could and should have made a proper disclosure when  
7 accepting hotel reservations, during the check-in process, or by any other means reasonably  
8 calculated to inform consumers of its inadequate data security.

9       209. Also, Nev. Rev. Stat. § 598.0923(3), which is encompassed by the Nevada  
10 Consumer Fraud Act quoted above, states: "A person engages in a 'deceptive trade practice' when  
11 in the course of his or her business or occupation he or she knowingly: . . . 3) Violates a state or  
12 federal statute or regulation relating to the sale or lease of . . . services." MGM violated this  
13 provision for several reasons, each of which serves as an independent act for purposes of violating  
14 § 598.0923(3).

15       210. *First*, MGM breached a Nevada statute requiring reasonable data security.  
16 Specifically, Nev. Rev. Stat. § 603A.210(1) states: "A data collector that maintains records which  
17 contain personal information of a resident of this State shall implement and maintain *reasonable*  
18 *security measures* to protect those records from unauthorized access [or] acquisition." (Emphasis  
19 added.) MGM is a data collector as defined at Nev. Rev. Stat. § 603A.030. MGM failed to  
20 implement and maintain reasonable security measures, evidenced by the fact that hackers accessed  
21 MGM's cloud server and stole consumers' PII. MGM's violation of this statute was done  
22 knowingly for purposes of Nev. Rev. Stat. § 598.0923(3) because MGM knew or should have  
23 known that its data security practices were deficient. This is true because, among other things,  
24 MGM was aware that the hotel industry was a frequent target of sophisticated cyberattacks. MGM  
25 knew or should have known that its data security practices were insufficient to guard against those  
26 attacks. MGM had knowledge of the facts that constituted the violation.

27       211. *Second*, MGM breached other state statutes regarding unfair trade practices and  
28

1 data security requirements as alleged *infra*. Specifically, MGM violated the state statutes set forth  
2 in Counts VI-XIV. MGM also violated Nev. Rev. Stat. § 598.0923(2) as alleged above in this  
3 Count. MGM knew or should have known that it violated these statutes. MGM’s violations of each  
4 of these statutes serves as a separate actionable act for purposes of violating Nev. Rev. Stat. §  
5 598.0923(3).

6 212. *Third*, MGM violated the FTC Act, 15 U.S.C. § 45, as alleged above. MGM knew  
7 or should have known that its data security practices were deficient, violated the FTC Act, and that  
8 it failed to adhere to the FTC’s data security guidance. This is true because, among other things,  
9 MGM was aware that the hotel industry was a frequent target of sophisticated cyberattacks. MGM  
10 knew or should have known that its data security practices were insufficient to guard against those  
11 attacks. MGM had knowledge of the facts that constituted the violation. MGM’s violation of the  
12 FTC Act serves as a separate actionable act for purposes of violating Nev. Rev. Stat. § 598.0923(3).

13 213. MGM engaged in deceptive or unfair practices by engaging in conduct that is  
14 contrary to public policy, unscrupulous, and caused injury to Plaintiffs and Class members.

15 214. Plaintiffs and Class members were denied a benefit conferred on them by the  
16 Nevada legislature.

17 215. Nevada Rev. Stat. § 41.600(3) states that if the plaintiffs prevail, the court “shall  
18 award: (a) Any damages that the claimant has sustained; (b) Any equitable relief that the court  
19 deems appropriate; and (c) the claimant’s costs in the action and reasonable attorney’s fees.”

20 216. As a direct and proximate result of the foregoing, Plaintiffs and Class members  
21 suffered all forms of damages alleged herein. Plaintiffs’ harms constitute compensable damages  
22 for purposes of Nev. Rev. Stat. § 41.600(3).

23 217. Plaintiffs and Class members are also entitled to all forms of injunctive relief sought  
24 herein.

25 218. Plaintiffs and Class members are also entitled to an award of their attorney’s fees  
26 and costs pursuant to Nev. Rev. Stat. § 41.600(3)(c).

1 **COUNT VI**  
2 **VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW (UCL)**  
3 **Cal. Bus. & Prof. Code §§ 17200, et seq.**  
4 **(On Behalf of the California Subclass)**

5 219. Plaintiffs Bohlim, Hwynn, Sedaghatpour, and Simkin (the “California Plaintiffs”) re-allege and incorporate by reference all preceding allegations as if fully set forth herein.

6 220. MGM and the California Plaintiffs are “persons” as defined by the California Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code § 17201.

7 221. The UCL states that “unfair competition shall mean and include any [1] unlawful, unfair or fraudulent business act or practice and [2] unfair, deceptive, untrue or misleading advertising.” Cal. Bus. & Prof. Code § 17200.

8 222. The first section of the UCL quoted above includes three separate prongs: “unlawful,” “unfair,” or “fraudulent” practices. MGM violated each of these prongs.

9 223. *First*, MGM engaged in “unlawful” acts or practices because it violated multiple laws, including but not limited to the California Consumer Records Act, Cal. Civ. Code § 1798.81.5 (requiring reasonable data security measures); the California Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq.; the FTC Act, 15 U.S.C. § 45; and the common law, all as alleged herein.

10 224. *Second*, MGM engaged in “unfair” acts or practices, including but not limited to the following:

11 (a) MGM failed to implement and maintain reasonable data security measures to protect the California Subclass members’ PII. MGM failed to identify foreseeable security risks, remediate identified risks, and adequately improve its data security in light of the known risk of cyber intrusions in the hotel industry. MGM’s conduct, with little if any social utility, is unfair when weighed against the harm to the California Subclass members whose PII has been compromised.

12 (b) MGM’s failure to implement and maintain reasonable data security measures was also contrary to legislatively-declared public policy that seeks to protect



1 consumers' personal information and ensure that entities entrusted with PII adopt  
2 appropriate security measures. These policies are reflected in various laws, including but  
3 not limited to the FTC Act, 15 U.S.C. § 45; and the California Consumer Records Act, Cal.  
4 Civ. Code § 1798.81.5 (requiring reasonable data security measures).

5 (c) MGM's failure to implement and maintain reasonable data security  
6 measures also led to substantial consumer injuries described herein, which are not  
7 outweighed by countervailing benefits to consumers or to competition. Moreover, because  
8 consumers could not know of MGM's inadequate data security, consumers could not have  
9 reasonably avoided the harms that MGM's conduct caused.

10 (d) Also, MGM retained consumers' PII for years after their original hotel  
11 stays, much longer than was necessary to achieve the goal of processing the consumers'  
12 hotel room rentals. As a result, MGM amassed an enormous trove of PII. Given the volume  
13 and sensitivity of PII within MGM's database, MGM should have taken adequate measures  
14 to protect the data. MGM failed to do so.

15 225. *Third*, MGM engaged in "fraudulent" acts or practices, including but not limited to  
16 the following:

17 (a) MGM omitted and concealed the fact that it did not employ reasonable  
18 safeguards to protect consumers' PII. MGM could and should have made a proper  
19 disclosure when accepting hotel reservations, during the check-in process, or by any other  
20 means reasonably calculated to inform consumers of the inadequate data security. MGM  
21 knew or should have known that its data security practices were deficient. This is true  
22 because, among other things, MGM was aware that the hotel industry was a frequent target  
23 of sophisticated cyberattacks. MGM knew or should have known that its data security was  
24 insufficient to guard against those attacks.

25 (b) MGM also made implied or implicit false representations that its data  
26 security practices were sufficient to protect consumers' PII. MGM required consumers to  
27 provide their PII during the reservation and/or check-in process. In doing so, MGM made  
28

1 implied or implicit representations that its data security practices were sufficient to protect  
2 consumers' PII. By virtue of accepting Plaintiffs' PII during the reservation and check-in  
3 process, MGM implicitly represented that its data security procedures were sufficient to  
4 safeguard the PII. Those representations were false and misleading.

5 (c) MGM retained consumers' PII for years after the original hotel stays, much  
6 longer than was necessary to achieve the goal of processing the consumers' hotel room  
7 rentals. As a result, MGM amassed an enormous trove of PII. Given the volume and  
8 sensitivity of PII within MGM's database, MGM knew that it should have taken adequate  
9 measures to protect the data. MGM failed to do so.

10 226. MGM's omissions and misrepresentations were material because they were likely  
11 to deceive reasonable consumers regarding the adequacy of MGM's data security.

12 227. MGM also engaged in "unfair, deceptive, untrue or misleading advertising" for  
13 purposes of Cal. Bus. & Prof. Code § 17200 for the following reasons:

14 (a) MGM omitted and concealed the fact that it did not employ reasonable  
15 safeguards to protect consumers' PII. MGM could and should have made a proper  
16 disclosure when accepting hotel reservations, during the check-in process, or by any other  
17 means reasonably calculated to inform consumers of the inadequate data security. MGM  
18 knew or should have known that its data security practices were deficient for the reasons  
19 noted above.

20 (b) MGM also made implied or implicit false representations that its data  
21 security practices were sufficient to protect consumers' PII. MGM required consumers to  
22 provide their PII during the reservation and/or check-in process. In doing so, MGM made  
23 implied or implicit representations that its data security practices were sufficient to protect  
24 consumers' PII. By virtue of accepting Plaintiffs' PII during the reservation and check-in  
25 process, MGM implicitly represented that its data security processes were sufficient to  
26 safeguard the PII. Those representations were unfair, deceptive, untrue, or misleading.

27 228. The California Plaintiffs and California Subclass members transacted with MGM  
28

1 in California by, among other things, making hotel reservations from California and paying any  
2 necessary room deposits from California. MGM acknowledges that “Southern California [is]  
3 where a large number of our customers reside.”<sup>58</sup> The California Plaintiffs and California Subclass  
4 members were deceived in California when they made reservations from California and were not  
5 informed of MGM’s deficient data security practices.

6 229. As a direct and proximate result of MGM’s unfair, unlawful, and fraudulent acts  
7 and practices, the California Plaintiffs and California Subclass members were injured, lost money  
8 or property, and suffered the various types of damages alleged herein.

9 230. The UCL states that an action may be brought by any person who has “suffered  
10 injury in fact and has lost money or property as a result of the unfair competition.” Cal. Bus. &  
11 Prof. Code §17204. The California Plaintiffs and California Subclass members suffered injury in  
12 fact and lost money or property as a result of MGM’s unfair competition as set forth herein. This  
13 includes, *e.g.*, the loss of value in their breached PII. PII is valuable, which is demonstrated not  
14 only by the fact that MGM requires consumers to provide PII during the reservation and check-in  
15 process, but also because MGM uses PII for its marketing and other purposes. Furthermore, PII  
16 stolen from MGM was marketed on the “dark web.” Due to MGM’s misconduct and the resulting  
17 Data Breach, hackers took this valuable PII without providing compensation to Plaintiffs and Class  
18 members.

19 231. Cal. Bus. & Prof. Code §17203 states:

20 Any person who engages, has engaged, or proposes to engage in unfair competition  
21 may be enjoined in any court of competent jurisdiction. The court may make such  
22 orders or judgments . . . as may be necessary to prevent the use or employment by  
23 any person of any practice which constitutes unfair competition, as defined in this  
24 chapter, or as may be necessary to restore to any person in interest any money or  
25 property, real or personal, which may have been acquired by means of such unfair  
26 competition.

---

26 <sup>58</sup> See MGM Resorts International Form 10-K for the year ended Dec. 31, 2019, at pg. 20, *available*  
27 *at* <http://d18rn0p25nwr6d.cloudfront.net/CIK-0000789570/7de59e1c-7d63-4df5-88a7-7e1ca2d0853d.pdf> (last visited Feb. 26, 2021).

1 232. The California Plaintiffs and California Subclass members are entitled to the  
2 injunctive relief requested herein to address MGM’s past and future acts of unfair competition.

3 233. The California Plaintiffs and California Subclass members are entitled to a  
4 restoration of money or property that was acquired by MGM by means of its unfair competition.

5 234. The California Plaintiffs and California Subclass members seek all monetary and  
6 non-monetary relief allowed by the UCL, including reasonable attorneys’ fees under Cal. Code of  
7 Civ. Procedure § 1021.5.

8 **COUNT VII**  
9 **VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT (CLRA)**  
10 **Cal. Civ. Code §§ 1750, *et seq.***  
11 **(On Behalf of the California Subclass)**

12 235. The California Plaintiffs re-allege and incorporate by reference all preceding  
13 allegations as if fully set forth herein.

14 236. The Consumers Legal Remedies Act (“CLRA”), Cal. Civ. Code §§ 1750, *et seq.*,  
15 is a comprehensive statutory scheme that is to be “liberally construed” to protect consumers against  
16 unfair and deceptive business practices by businesses providing goods or services to consumers.  
17 Cal. Civ. Code § 1760.

18 237. MGM is a “person” as defined in Cal. Civ. Code § 1761(c).

19 238. The California Plaintiffs and California Subclass members are “consumers” as  
20 defined in Cal. Civ. Code § 1761(d).

21 239. MGM has provided “services” as defined in Cal. Civ. Code § 1761(b).

22 240. The California Plaintiffs and California Subclass members have engaged in  
23 “transactions” as defined in Civil Code § 1761(e).

24 241. Cal. Civ. Code § 1770(a) states:

25 (a) The following unfair methods of competition and unfair or deceptive acts or  
26 practices undertaken by any person in a transaction . . . that results in the sale or  
27 lease of goods or services to any consumer are unlawful:

28 . . . .

(5) Representing that goods or services have . . . characteristics, . . . uses,

1 [or] benefits . . . that they do not have . . . [or]

2 . . . .

3 (7) Representing that goods or services are of a particular standard, quality,  
4 or grade . . . if they are of another.

5 242. MGM's acts and practices resulted in the sale of services that violated Cal. Civil  
6 Code § 1770(a)(5) and (7).

7 243. Omissions are actionable under Cal. Civil Code § 1770(a)(5) and (7).

8 244. MGM's unlawful acts included the following:

9 (a) MGM omitted and concealed the fact that it did not employ reasonable  
10 safeguards to protect consumers' PII. MGM could and should have made a proper  
11 disclosure when accepting hotel reservations, during the check-in process, or by any other  
12 means reasonably calculated to inform consumers of the inadequate data security. MGM  
13 knew or should have known that its data security practices were deficient. This is true  
14 because, among other things, MGM was aware that the hotel industry was a frequent target  
15 of sophisticated cyberattacks. MGM knew or should have known that its data security was  
16 insufficient to guard against those attacks.

17 (b) MGM also made implied or implicit representations that its data security  
18 practices were sufficient to protect consumers' PII. MGM required consumers to provide  
19 their PII during the reservation and/or check-in process. In doing so, MGM made implied  
20 or implicit representations that its data security practices were sufficient to protect  
21 consumers' PII. By virtue of accepting Plaintiffs' PII during the reservation and check-in  
22 process, MGM implicitly represented that its data security processes were sufficient to  
23 safeguard the PII. Those representations were false and misleading.

24 245. MGM's misrepresentations and omissions were material because they were likely  
25 to and did deceive reasonable consumers about the adequacy of MGM's data security and ability  
26 to protect the confidentiality of consumers' PII.

27 246. Had MGM disclosed to the California Plaintiffs and California Subclass members  
28

1 that its data systems were not reasonably secure, MGM would have been unable to continue in  
2 business in like fashion and it would have been forced to adopt reasonable data security measures.  
3 Instead, MGM received, maintained, and compiled Class members' PII as part of the services  
4 MGM provided and for which Class members paid, without advising Class members that MGM's  
5 data security practices were insufficient to protect the PII.

6 247. The California Plaintiffs and California Subclass members transacted with MGM  
7 in California by, among other things, making hotel reservations from California and paying any  
8 necessary room deposits from California. MGM acknowledges that "Southern California [is]  
9 where a large number of our customers reside."<sup>59</sup> The California Plaintiffs and California Subclass  
10 members were deceived in California when they made reservations from California and were not  
11 informed of MGM's deficient data security practices.

12 248. Cal. Civ. Code § 1780(a) states:

13 Any consumer who suffers any damage as a result of the use or employment by any  
14 person of a method, act, or practice declared to be unlawful by Section 1770 may  
bring an action against that person to recover or obtain any of the following:

- 15 (1) Actual damages, but in no case shall the total award of damages in a  
16 class action be less than one thousand dollars (\$1,000).
- 17 (2) An order enjoining the methods, acts, or practices.
- 18 (3) Restitution of property.
- 19 (4) Punitive damages.
- 20 (5) Any other relief that the court deems proper.

21 249. Plaintiffs suffered "damages" and "actual damages" based on the various damages  
22 alleged herein.

23 250. Plaintiffs are entitled to the injunctive relief sought herein to enjoin MGM's  
24

---

25  
26 <sup>59</sup> See MGM Resorts International Form 10-K for the year ended Dec. 31, 2019, at pg. 20, available  
27 at <http://d18rn0p25nwr6d.cloudfront.net/CIK-0000789570/7de59e1c-7d63-4df5-88a7-7e1ca2d0853d.pdf> (last visited Feb. 26, 2021).

1 unlawful methods, acts, or practices.

2       251. Plaintiffs are entitled to “restitution of property,” including but not limited to the  
3 value of monies they overpaid to MGM for its services and the value of the PII they provided to  
4 MGM.

5       252. Plaintiffs are also entitled to punitive damages under Cal. Civ. Code § 1780(a)(4).  
6 MGM knew or should have known that its data security practices were deficient. This is true  
7 because, among other things, MGM was aware that the hotel industry was a frequent target of  
8 sophisticated cyberattacks. MGM knew or should have known that its data security was  
9 insufficient to guard against those attacks. Also, given the size of MGM’s database and the  
10 sensitivity of the PII therein, MGM should have taken adequate measures to protect the data. MGM  
11 intentionally failed to encrypt the PII while it was stored on MGM’s server. Also, MGM  
12 intentionally retained consumers’ PII for years after their original hotel stays, much longer than  
13 was necessary to achieve the goal of processing the consumers’ transactions.

14       253. Cal. Civ. Code § 1780(e) states that the “court shall award court costs and attorney’s  
15 fees to a prevailing plaintiff in litigation filed pursuant to this section.” Plaintiffs are entitled to an  
16 award of attorney’s fees and costs.

17       254. MGM’s violations of the CLRA were not the result of a “bona fide error” for  
18 purposes of Cal Civ. Code § 1784. Instead, MGM acted with knowledge, recklessness, gross  
19 negligence, negligence, and/or any other form of actionable misconduct.

20       255. As a result of MGM’s violations of Cal. Civ. Code § 1770(a)(5) and (7), the  
21 California Plaintiffs and California Subclass members have suffered and will continue to suffer  
22 injury, ascertainable losses of money or property, and monetary and non-monetary damages of the  
23 various types alleged herein.

24       256. The California Plaintiffs and California Subclass members seek all monetary and  
25 non-monetary relief allowed under the CLRA, including injunctive relief enjoining the acts and  
26 practices described above.

27       257. Plaintiffs satisfy all requirements for class action treatment set forth in Cal. Civ.  
28

1 Code § 1781(b). As discussed more fully above in the Class Action Allegations section, it is  
2 impracticable to bring all members of the California Subclass before the court. The questions of  
3 law or fact common to the class are substantially similar for each Class member, and they  
4 predominate over any questions affecting individual Class members. The claims of the California  
5 Plaintiffs are typical of the claims of the California Subclass. The California Plaintiffs will fairly  
6 and adequately represent the interests of the California Subclass.

7 258. The California Plaintiffs have provided timely notice to MGM of their claims for  
8 damages under the CLRA, in compliance with Cal. Civ. Code § 1782(a).

9 **COUNT VIII**  
10 **VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT (CCRA)**  
11 **Cal. Civ. Code §§ 1798.80, *et seq.***  
**(On Behalf of the California Subclass)**

12 259. The California Plaintiffs re-allege and incorporate by reference all preceding  
13 allegations as if fully set forth herein.

14 260. The California legislature enacted the California Customer Records Act (“CCRA”)  
15 to “ensure that personal information about California residents is protected.” Cal. Civ. Code §  
16 1798.81.5.

17 261. The CCRA states: “A business that owns, licenses, or maintains personal  
18 information about a California resident shall implement and maintain *reasonable security*  
19 *procedures and practices* appropriate to the nature of the information, to protect the personal  
20 information from unauthorized access . . . .” Cal. Civ. Code § 1798.81.5(b) (emphasis added).

21 262. The CCRA defines owns, licenses, and maintains as follows: “[T]he terms ‘own’  
22 and ‘license’ include personal information that a business retains as part of the business’ internal  
23 customer account or for the purpose of using that information in transactions with the person to  
24 whom the information relates. The term ‘maintain’ includes personal information that a business  
25 maintains but does not own or license.” Cal. Civ. Code § 1798.81.5(a)(2). MGM owns, licenses,  
26 and/or maintains the PII that was involved in the Data Breach.

27 263. The CCRA defines personal information as follows: “‘Personal information’ means  
28



1 either of the following: (A) An individual’s first name of first initial and the individual’s last name,  
2 in combination with any one or more of the following data elements, when either the name or the  
3 data elements are not encrypted or redacted: . . . (ii) Driver’s license number, . . . passport number,  
4 [or] military identification number . . . .” Cal. Civ. Code § 1798.81.5(d)(1)(A)(ii). The PII stolen  
5 in the Data Breach includes personal information that meets this definition. The PII was  
6 unencrypted, evidenced by the fact that it was posted to the dark web in a readable form. Each of  
7 the California Plaintiffs (Messrs. Bohlim, Hwynn, Sedaghatpour, and Simkin) presented their  
8 driver’s license number to MGM when checking in for one or more of their hotel stays, thus MGM  
9 possessed their driver’s license numbers.

10 264. MGM failed to maintain reasonable data security procedures appropriate to the  
11 nature of the PII. Accordingly, MGM violated Cal. Civ. Code § 1798.81.5(b).

12 265. The California Plaintiffs and California Subclass members were “injured” by  
13 MGM’s violation of Cal. Civ. Code § 1798.81.5(b) and seek “damages” pursuant to Cal. Civ. Code  
14 § 1798.84(b). The California Plaintiffs and California Subclass members were injured in the  
15 various ways alleged herein. They seek all monetary and non-monetary relief allowed by the  
16 CCRA to compensate for their various types of damages alleged herein.

17 266. The California Plaintiffs and California Subclass members are also entitled to  
18 injunctive relief pursuant to Cal. Civ. Code § 1798.84(e), including but not limited to substantial  
19 improvements to MGM’s data security systems and all other injunctive remedies sought herein.

20 **COUNT IX**  
21 **VIOLATION OF THE CONNECTICUT UNFAIR TRADE PRACTICES ACT**  
22 **Conn. Gen. Stat. § 42-110a, et seq.**  
**(On Behalf of the Connecticut Subclass)**

23 267. Plaintiff Robert Taylor (“Plaintiff” for purposes of this count) re-alleges and  
24 incorporates by reference all preceding allegations as if fully set forth herein.

25 268. MGM, Plaintiff, and the Connecticut Subclass members are “persons” within the  
26 meaning of the Connecticut Unfair Trade Practices Act (“Conn. UTPA”), Conn. Gen. Stat. § 42-  
27 110a(3).

1           269. The Conn. UTPA states: “No person shall engage in unfair methods of competition  
2 and unfair or deceptive acts or practices in the conduct of any trade or commerce.” Conn. Gen.  
3 Stat. § 42-110b(a).

4           270. MGM engaged in unfair or deceptive acts or practices in violation of Conn. Gen.  
5 Stat. § 42-110b(a) by, among other things:

6           (a) Failing to adopt reasonable data security procedures to adequately  
7 safeguard consumers’ PII;

8           (b) Retaining PII for much longer than was necessary to process consumers’  
9 hotel stays;

10           (c) Omitting and concealing the material fact that it did not employ reasonable  
11 measures to secure consumers’ PII. MGM could and should have made a proper disclosure  
12 when accepting hotel reservations, during the check-in process, or by any other means  
13 reasonably calculated to inform consumers of the inadequate data security;

14           (d) Making implied or implicit representations that its data security practices  
15 were sufficient to protect consumers’ PII. MGM required consumers to provide their PII  
16 during the reservation and/or check-in process. In doing so, MGM made implied or implicit  
17 representations that its data security practices were sufficient to protect consumers’ PII. By  
18 virtue of accepting Plaintiffs’ PII during the reservation and check-in process, MGM  
19 implicitly represented that its data security processes were sufficient to safeguard the PII;  
20 and

21           (e) Failing to comply with common law and statutory duties pertaining to the  
22 security and privacy of Plaintiff and Connecticut Subclass members’ PII.

23           271. The Conn. UTPA states that its construction shall be “guided by interpretations  
24 given by the Federal Trade Commission and the federal courts to Section 5(a)(1) of the Federal  
25 Trade Commission Act (15 USC 45(a)(1)).” Conn. Gen. Stat. § 42-110b(b). As discussed *supra*,  
26 the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice  
27 prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

1 272. MGM conducted business in Connecticut for purposes of this claim. Connecticut  
2 Subclass members transacted with MGM in Connecticut by, among other things, making hotel  
3 reservations from Connecticut and paying any necessary room deposits from Connecticut. Plaintiff  
4 and the Connecticut Subclass members were deceived in Connecticut when they made reservations  
5 from Connecticut and were not informed of MGM's deficient data security practices.

6 273. The Conn. UTPA states the following at Conn. Gen. Stat. § 42-110g(a):

7 Any person who suffers any ascertainable loss of money or property, real or  
8 personal, as a result of the use or employment of a method, act or practice prohibited  
9 by section 42-110b, may bring an action . . . to recover actual damages. . . . The  
10 court may, in its discretion, award punitive damages and may provide such  
11 equitable relief as it deems necessary or proper.

12 274. Plaintiff and the Connecticut Subclass suffered an "ascertainable loss of money or  
13 property" based on the various types of damages alleged herein, including the loss of their PII.

14 275. Plaintiff and the Connecticut Subclass suffered "actual damages" based on the  
15 various types of damages alleged herein.

16 276. Plaintiffs are entitled to punitive damages under Conn. Gen. Stat. § 42-110g(a).  
17 MGM knew or should have known that its data security practices were deficient. This is true  
18 because, among other things, MGM was aware that the hotel industry was a frequent target of  
19 sophisticated cyberattacks. MGM knew or should have known that its data security was  
20 insufficient to guard against those attacks. Also, given the size of MGM's database and the  
21 sensitivity of the PII therein, MGM should have taken adequate measures to protect the data. MGM  
22 intentionally failed to encrypt the PII while it was stored on MGM's server. Also, MGM  
23 intentionally retained consumers' PII for years after the original hotel stays, much longer than was  
24 necessary to achieve the goal of processing the consumers' transactions.

25 277. Plaintiff and the Connecticut Subclass are entitled to the injunctive relief sought  
26 herein because, among other things, MGM continues to retain their PII and may subject that PII to  
27 further data breaches unless the requested injunctive relief is granted.

28 278. The Conn. UTPA permits claims to be brought as class actions. Conn. Gen. Stat. §  
42-110g(b).

1 279. The Conn. UTPA states the following at Conn. Gen. Stat. § 42-110g(d):

2 [T]he court may award, to the plaintiff . . . costs and reasonable attorneys’ fees  
3 based on the work reasonably performed by an attorney and not on the amount of  
4 recovery. . . . In any action brought under this section, the court may, in its  
5 discretion, order, in addition to damages or in lieu of damages, injunctive or other  
6 equitable relief.

7 280. Plaintiff and the Connecticut Subclass are entitled to recovery of their costs and  
8 reasonable attorneys’ fees.

9 281. As a result of MGM’s unfair or deceptive acts or practices, Plaintiff and the  
10 Connecticut Subclass have suffered and will continue to suffer ascertainable losses of money or  
11 property, as well as non-monetary damages, all as alleged herein.

12 282. Plaintiff and the Connecticut Subclass seek all monetary, non-monetary, and  
13 injunctive relief allowed by the Conn. UTPA.

14 **COUNT X**  
15 **VIOLATION OF THE GEORGIA DECEPTIVE TRADE PRACTICES ACT**  
16 **Ga. Code Ann. §§ 10-1-370, *et seq.***  
17 **(On Behalf of the Georgia Subclass)**

18 283. Plaintiff Fossett (“Plaintiff” for purposes of this count) re-alleges and incorporates  
19 by reference all preceding allegations as if fully set forth herein.

20 284. MGM, Plaintiff, and the Georgia Subclass members are “persons” within the  
21 meaning of the Georgia Deceptive Trade Practices Act (“Georgia DTPA”), Ga. Code Ann. § 10-  
22 1-370(5).

23 285. The Georgia DTPA states the following at Ga. Code Ann. § 10-1-372:

24 (a) A person engages in a deceptive trade practice when, in the course of his  
25 business, vocation, or occupation, he: . . . (5) Represents that goods or services  
26 have . . . characteristics, . . . uses, [or] benefits . . . that they do not have; . . . (7)  
27 Represents that goods or services are of a particular standard, quality, or grade . . .  
28 if they are of another; . . . [or] (12) Engages in any other conduct which similarly  
creates a likelihood of confusion or of misunderstanding.

285. MGM engaged in deceptive trade practices in violation of Ga. Code Ann. § 10-1-  
372(a)(5), (7), and (12) by, among other things:

(a) Omitting and concealing the material fact that it did not employ reasonable

1 measures to secure consumers' PII. MGM could and should have made a proper disclosure  
2 when accepting hotel reservations, during the check-in process, or by any other means  
3 reasonably calculated to inform consumers of the inadequate data security; and

4 (b) Making implied or implicit representations that its data security practices  
5 were sufficient to protect consumers' PII. MGM required consumers to provide their PII  
6 during the reservation and/or check-in process. In doing so, MGM made implied or implicit  
7 representations that its data security practices were sufficient to protect consumers' PII. By  
8 virtue of accepting Plaintiffs' PII during the reservation and check-in process, MGM  
9 implicitly represented that its data security processes were sufficient to safeguard the PII.

10 287. The Georgia DTPA states that "[i]n order to prevail in an action under this part, a  
11 complainant need not prove . . . actual confusion or misunderstanding." Ga. Code Ann. § 10-1-  
12 372(b).

13 288. The Georgia DTPA further states: "A person likely to be damaged by a deceptive  
14 trade practice of another may be granted an injunction against it under the principles of equity and  
15 on terms that the court considers reasonable. Proof of monetary damage, loss of profits, or intent  
16 to deceive is not required." Ga. Code Ann. § 10-1-373(a). Plaintiff and the Georgia Subclass are  
17 entitled to the injunctive relief sought herein because, among other things, MGM continues to  
18 retain their PII and may subject that PII to further data breaches unless the requested injunctive  
19 relief is granted.

20 289. The Georgia DTPA states that the "court, in its discretion, may award attorney's  
21 fees to the prevailing party if . . . [t]he party charged with a deceptive trade practice has willfully  
22 engaged in the trade practice knowing it to be deceptive." Ga. Code Ann. § 10-1-373(b)(2). MGM  
23 willfully engaged in deceptive trade practices knowing them to be deceptive. MGM knew or  
24 should have known that its data security practices were deficient. This is true because, among other  
25 things, MGM was aware that the hotel industry was a frequent target of sophisticated cyberattacks.  
26 MGM knew or should have known that its data security practices were insufficient to guard against  
27 those attacks.

1           290. The Georgia DTPA states that “[c]osts shall be allowed to the prevailing party  
2 unless the court otherwise directs.” Ga. Code Ann. § 10-1-373(b). Plaintiff and the Georgia  
3 Subclass are entitled to recover their costs of pursuing this litigation.

4           291. As a result of MGM’s deceptive acts and practices, Plaintiff and the Georgia  
5 Subclass have suffered and will continue to suffer injury, ascertainable losses of money or  
6 property, and non-monetary damages, as alleged herein.

7           292. Plaintiff and the Georgia Subclass seek all monetary and non-monetary relief  
8 allowed by the Georgia DTPA, including injunctive relief and attorneys’ fees.

9                               **COUNT XI**  
10                              **VIOLATION OF NEW YORK GENERAL BUSINESS LAW**  
11                                   **N.Y. Gen. Bus. Law § 349**  
                                  **(On Behalf of the New York Subclass)**

12           293. Plaintiff Kerri Shapiro (“Plaintiff” for purposes of this count) re-alleges and  
13 incorporates by reference all preceding allegations as if fully set forth herein.

14           294. New York Gen. Bus. Law § 349(a) states: “Deceptive acts or practices in the  
15 conduct of any business, trade or commerce or in the furnishing of any service in this state are  
16 hereby declared unlawful.”

17           295. MGM engaged in deceptive acts or practices in violation of N.Y. Gen. Bus. Law §  
18 349(a) by, among other things:

19               (a) Omitting and concealing the material fact that it did not employ reasonable  
20 measures to secure consumers’ PII. MGM could and should have made a proper disclosure  
21 when accepting hotel reservations, during the check-in process, or by any other means  
22 reasonably calculated to inform consumers of the inadequate data security;

23               (b) Making implied or implicit representations that its data security practices  
24 were sufficient to protect consumers’ PII. MGM required consumers to provide their PII  
25 during the reservation and/or check-in process. In doing so, MGM made implied or implicit  
26 representations that its data security practices were sufficient to protect consumers’ PII. By  
27 virtue of accepting Plaintiffs’ PII during the reservation and check-in process, MGM  
28

1 implicitly represented that its data security processes were sufficient to safeguard the PII;

2 (c) Failing to adopt reasonable safeguards to protect the New York Subclass  
3 members' PII in violation of N.Y. Gen. Bus. Law § 899-bb, which states: "Any person or  
4 business that owns or licenses computerized data which includes private information of a  
5 resident of New York shall develop, implement and maintain reasonable safeguards to  
6 protect the security, confidentiality and integrity of the private information. . . . Any person  
7 or business that fails to comply with this subdivision shall be deemed to have violated  
8 section three hundred forty-nine of this chapter."; and

9 (d) Omitting and concealing the material fact that it did not comply with  
10 common law and statutory duties pertaining to data security, including but not limited to  
11 duties imposed by the FTC Act, 15 U.S.C. § 45.

12 296. MGM conducted business in New York for purposes of this claim. New York  
13 Subclass members transacted with MGM in New York by, among other things, making hotel  
14 reservations from New York and paying any necessary room deposits from New York. Plaintiff  
15 and the New York Subclass members were deceived in New York when they made reservations  
16 from New York and were not informed of MGM's deficient data security practices.

17 297. MGM's omissions and misrepresentations were objectively likely to mislead a  
18 reasonable consumer acting reasonably under the circumstances.

19 298. MGM's omissions and misrepresentations were material because they were likely  
20 to deceive consumers regarding the adequacy of MGM's data security practices.

21 299. N.Y. Gen. Bus. Law § 349(h) states:

22 [A]ny person who has been injured by reason of any violation of this section may  
23 bring an action in his own name to enjoin such unlawful act or practice, an action  
24 to recover his actual damages or fifty dollars, whichever is greater, or both such  
25 actions. The court may, in its discretion, increase the award of damages to an  
26 amount not to exceed three times the actual damages up to one thousand dollars, if  
the court finds the defendant willfully or knowingly violated this section. The court  
may award reasonable attorney's fees to a prevailing plaintiff.

27 300. The various types of damages incurred by Plaintiff and the New York Subclass  
28

1 alleged herein satisfy both the “injured” and “actual damages” requirements of N.Y. Gen. Bus.  
2 Law § 349(h). Plaintiff and the New York Subclass suffered and will continue to suffer injury, loss  
3 of money or property, and monetary and non-monetary damages, as alleged herein. Plaintiff and  
4 the New York Subclass members are entitled to the greater of their actual damages or statutory  
5 damages of \$50.

6 301. Plaintiff and the New York Subclass are entitled to treble damages of up to \$1,000  
7 under N.Y. Gen. Bus. Law § 349(h) because MGM “willfully or knowingly” violated N.Y. Gen.  
8 Bus. Law § 349(a). MGM knew or should have known that its data security practices were  
9 deficient. This is true because, among other things, MGM was aware that the hotel industry was a  
10 frequent target of sophisticated cyberattacks. MGM knew or should have known that its data  
11 security practices were insufficient to guard against those attacks. Given the volume and sensitivity  
12 of the PII in MGM’s database, MGM should have taken adequate measures to protect the data and  
13 should have been aware of any shortcomings. MGM also willfully and knowingly failed to encrypt  
14 the PII. MGM also willfully and knowingly retained consumers’ PII for much longer than was  
15 necessary to process the underlying hotel stays.

16 302. MGM’s deceptive and unlawful practices affected the public interest and  
17 consumers at large, including thousands or more of New York residents affected by the Data  
18 Breach.

19 303. MGM’s deceptive and unlawful practices caused substantial injury to Plaintiff and  
20 New York Subclass members that those individuals could not reasonably avoid.

21 304. Plaintiff and the New York Subclass are entitled to the injunctive relief sought  
22 herein because, among other things, MGM continues to retain their PII and may subject that PII to  
23 further data breaches unless injunctive relief is granted.

24 305. Plaintiff and the New York Subclass are entitled to an award of their attorney’s fees  
25 under N.Y. Gen. Bus. Law § 349(h).

26  
27  
28



1 **COUNT XII**  
2 **VIOLATION OF THE OHIO DECEPTIVE TRADE PRACTICES ACT**  
3 **Ohio Rev. Code §§ 4165.01, et seq.**  
4 **(On Behalf of the Ohio Subclass)**

5 306. Plaintiff Julie Mutsko (“Plaintiff” for purposes of this count) re-alleges and  
6 incorporates by reference all preceding allegations as if fully set forth herein.

7 307. MGM, Plaintiff, and Ohio Subclass members are each a “person” as defined in  
8 Ohio Rev. Code § 4165.01(D).

9 308. The Ohio Deceptive Trade Practices Act states: “A person engages in a deceptive  
10 trade practice when, in the course of the person’s business, vocation, or occupation, the person  
11 does any of the following: . . . (7) Represents that goods or services have . . . characteristics . . .  
12 [or] benefits . . . that they do not have; . . . [or] (9) Represents that goods or services are of a  
13 particular standard [or] quality . . . if they are of another.” Ohio Rev. Code § 4165.02(A)(7), (9).

14 309. MGM engaged in deceptive trade practices in violation of Ohio Rev. Code §  
15 4165.02(A)(7) and (9) by:

16 (a) Omitting and concealing the material fact that it did not employ reasonable  
17 measures to secure consumers’ PII. MGM could and should have made a proper disclosure  
18 when accepting hotel reservations, during the check-in process, or by any other means  
19 reasonably calculated to inform consumers of the inadequate data security;

20 (b) Making implied or implicit representations that its data security practices  
21 were sufficient to protect consumers’ PII. MGM required consumers to provide their PII  
22 during the reservation and/or check-in process. In doing so, MGM made implied or implicit  
23 representations that its data security practices were sufficient to protect consumers’ PII. By  
24 virtue of accepting Plaintiffs’ PII during the reservation and check-in process, MGM  
25 implicitly represented that its data security processes were sufficient to safeguard the PII;  
26 and

27 (c) Omitting that it did not comply with common law and statutory duties  
28 pertaining to the security of PII, including but not limited to duties imposed by the FTC

1 Act, 15 U.S.C. § 45.

2 310. MGM’s representations and omissions were material because they were likely to  
3 deceive reasonable consumers about the adequacy of MGM’s data security and ability to protect  
4 the confidentiality of consumers’ PII.

5 311. MGM advertised, offered, or sold goods or services in Ohio and engaged in trade  
6 or commerce directly or indirectly affecting the people of Ohio.

7 312. Plaintiff and the Ohio Subclass members transacted with MGM in Ohio by, among  
8 other things, making hotel reservations from Ohio and paying any necessary room deposits from  
9 Ohio. Plaintiff and the Ohio Subclass members were deceived in Ohio when they made  
10 reservations from Ohio and were not informed of MGM’s deficient data security practices.

11 313. Ohio Rev. Code § 4165.03(B) states that an “award of attorney’s fees may be  
12 assessed against a defendant if the court finds that the defendant has willfully engaged in a trade  
13 practice listed in division (A) of section 4165.02 of the Revised Code knowing it to be deceptive.”  
14 MGM willfully engaged in its deceptive conduct knowing it to be deceptive. MGM knew or should  
15 have known that its data security practices were deficient. This is true because, among other things,  
16 MGM was aware that the hotel industry was a frequent target of sophisticated cyberattacks. MGM  
17 knew or should have known that its data security practices were insufficient to guard against those  
18 attacks.

19 314. As a direct and proximate result of MGM’s deceptive trade practices, Plaintiff and  
20 the Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses  
21 of money or property, and monetary and non-monetary damages as alleged herein.

22 315. Plaintiff and the Ohio Subclass members seek all monetary and non-monetary relief  
23 allowed by law, including actual damages, restitution, injunctive relief, attorneys’ fees, and any  
24 other relief available under Ohio Rev. Code § 4165.03.

25  
26  
27  
28

1 **COUNT XIII**  
2 **VIOLATION OF THE OREGON UNLAWFUL TRADE PRACTICES ACT**  
3 **Ore. Stat. §§ 646.605, et seq.**  
4 **(On Behalf of the Oregon Subclass)**

5 316. Plaintiff Dvorak (“Plaintiff” for purposes of this count) re-alleges and incorporates  
6 by reference all preceding allegations as if fully set forth herein.

7 317. MGM, Plaintiff, and Oregon Subclass members are “persons” within the meaning  
8 of the Oregon Unlawful Trade Practices Act (“Oregon UTPA”), Ore. Stat. § 646.605(4).

9 318. MGM engaged in “trade” or “commerce” within the meaning of Ore. Stat. §  
646.605(8).

10 319. The Oregon UTPA, at Ore. Stat. § 646.608, states the following:

11 (1) A person engages in an unlawful practice if in the course of the person’s  
12 business, vocation or occupation the person does any of the following: . . . (e)  
13 Represents that . . . goods or services have . . . characteristics, . . . benefits, . . . or  
14 qualities that the . . . goods or services do not have . . . . (g) Represents that . . .  
15 goods or services are of a particular standard, quality, or grade . . . if the . . . goods  
16 or services are of another. . . . [or] (u) Engages in any other unfair or deceptive  
17 conduct in trade or commerce.

18 320. Ore. Stat. § 646.608(2) states that a “representation under subsection (1) of this  
19 section . . . may be any manifestation of any assertion by words or conduct, including, but not  
20 limited to, a failure to disclose a fact.”

21 321. MGM engaged in deceptive or unfair practices in violation of Ore. Stat. §  
22 646.608(1)(e), (g), and (u) by, among other things:

23 (a) Omitting and concealing the material fact that it did not employ reasonable  
24 measures to secure consumers’ PII. MGM could and should have made a proper disclosure  
25 when accepting hotel reservations, during the check-in process, or by any other means  
26 reasonably calculated to inform consumers of the inadequate data security;

27 (b) Making implied or implicit representations that its data security practices  
28 were sufficient to protect consumers’ PII. MGM required consumers to provide their PII  
during the reservation and/or check-in process. In doing so, MGM made implied or implicit  
representations that its data security practices were sufficient to protect consumers’ PII. By

1 virtue of accepting Plaintiffs’ PII during the reservation and check-in process, MGM  
2 implicitly represented that its data security processes were sufficient to safeguard the PII;

3 (c) Omitting that it did not comply with common law and statutory duties  
4 pertaining to the security of PII, including but not limited to duties imposed by the FTC  
5 Act, 15 U.S.C. § 45;

6 (d) Failing to implement reasonable data security measures to protect  
7 consumers’ PII; and

8 (e) Retaining PII for much longer than was necessary to process consumers’  
9 hotel stays.

10 322. The Oregon UTPA also states: “A person engages in an unlawful trade practice if  
11 in the course of the person’s business, vocation or occupation the person: . . . (9) Violates a  
12 provision of ORS 646A.600 to 646A.628.” Ore. Stat. § 646.607(9). MGM violated two relevant  
13 sections of ORS 646A.600 to 646A.628.

14 (a) *First*, MGM violated Ore. Stat. § 646A.622(1), which states that entities  
15 that hold consumer data “shall develop, implement and maintain *reasonable safeguards* to  
16 protect the security, confidentiality and integrity of personal information.” (Emphasis  
17 added.) MGM’s violation of this code section is set forth more fully in the following Count,  
18 *infra*. MGM’s violation of Ore. Stat. § 646A.622(1) serves as an independent actionable  
19 act for purposes of Plaintiff’s Oregon UTPA claim under Ore. Stat. § 646.607. *See* Ore.  
20 Stat. § 646A.604(11)(a) (“A person’s violation of a provision of [the reasonable safeguards  
21 requirement of § 646A.622(1)] is an unlawful practice under ORS 646.607.”).

22 (b) *Second*, MGM violated Ore. Stat. § 646A.604(1), which states: “If a  
23 covered entity is subject to a breach of security . . . , the covered entity shall give notice of  
24 the breach of security to: (a) The consumer to whom the personal information pertains.”  
25 The entity “shall give notice of a breach of security in the most expeditious manner  
26 possible, without unreasonable delay.” Ore. Stat. § 646A.604(3)(a). MGM failed to  
27 disclose the Data Breach in a timely manner. The hackers stole PII from MGM on July 7,  
28

1 2019, and MGM discovered the breach on July 10, 2019. MGM did not begin sending  
2 notices to affected consumers until two months later, on or around September 7, 2019.  
3 MGM has offered no explanation the delay. The length of the delay was unreasonable. The  
4 delay deprived Plaintiff and Oregon Subclass members of the ability to take prompt steps  
5 to closely scrutinize their financial and other accounts and take other protective measures  
6 to detect and deter misuse of their data. Also, MGM notified only a small fraction of the  
7 Oregon Subclass. To this day, MGM still has not notified many – perhaps most – of the  
8 affected consumers. In the days and months following the Data Breach, MGM did not post  
9 any announcements of the Data Breach on its website or issue any press releases  
10 announcing the breach. By failing to disclose the Data Breach in a timely manner, MGM  
11 violated Ore. Stat. § 646A.604(1) and (3)(a). MGM’s violation of Ore. Stat. § 646A.604  
12 serves as an independent actionable act for purposes of Plaintiff’s Oregon UTPA claim  
13 under Ore. Stat. § 646.607. *See* Ore. Stat. § 646A.604(11)(a) (“A person’s violation of a  
14 provision of [the data breach notification requirement of § 646A.604] is an unlawful  
15 practice under ORS 646.607.”).

16 323. The Oregon UTPA also states: “A person engages in an unlawful trade practice if  
17 in the course of the person’s business, vocation or occupation the person: (1) Employs any  
18 unconscionable tactic in connection with selling [or] renting . . . goods or services.” Ore. Stat. §  
19 646.607(1).

20 324. MGM employed unconscionable tactics. MGM knew or should have known that  
21 its data security practices were deficient. This is true because, among other things, MGM was  
22 aware that the hotel industry was a frequent target of sophisticated cyberattacks. MGM knew or  
23 should have known that its data security was insufficient to guard against those attacks. Also, given  
24 the volume and sensitivity of the PII in MGM’s database, MGM should have taken adequate  
25 measures to protect the data. MGM also knowingly failed to encrypt the PII stored on its server.  
26 Further, MGM retained consumers’ PII for years after the original hotel stays, much longer than  
27 was necessary to achieve the goal of processing the consumers’ transactions.  
28

1 325. Ore. Stat. § 646.638(1) states:

2 [A] person that suffers an ascertainable loss of money or property, real or personal,  
3 as a result of another person’s willful use or employment of a method, act or  
4 practice declared unlawful under ORS 646.608, may bring an individual action in  
5 an appropriate court to recover actual damages or statutory damages of \$200,  
6 whichever is greater. The court or the jury may award punitive damages and the  
7 court may provide any equitable relief the court considers necessary or proper.

8 326. Willful conduct is defined as follows: “A willful violation occurs when the person  
9 committing the violation knew or should have known that the conduct of the person was a  
10 violation.” Ore. Stat. 646.605(10). MGM engaged in a willful violation of the Oregon UTPA for  
11 the reasons noted above regarding MGM’s unconscionable tactics. As a result, Plaintiff and the  
12 Oregon Subclass members are entitled to the greater of their actual damages or statutory damages  
13 of \$200 pursuant to Ore. Stat. § 646.638(1).

14 327. Punitive damages are also warranted under Ore. Stat. § 646.638(1), for the same  
15 reasons discussed above regarding MGM’s unconscionable tactics.

16 328. Plaintiff and the Oregon Subclass suffered an “ascertainable loss of money or  
17 property” based on the various types of damages alleged herein, including the loss of their PII.

18 329. Ore. Stat. § 646.638(3) states that the “court may award reasonable attorney fees  
19 and costs at trial and on appeal to a prevailing plaintiff in an action under this section.” Plaintiff  
20 and the Oregon Subclass seek an award of their attorney fees and costs.

21 330. Ore. Stat. § 646.638(8) expressly permits class actions and the recovery therein of  
22 statutory damages, punitive damages, and injunctive relief:

23 A class action may be maintained under this section. In any class action under this  
24 section:

25 (a) Statutory damages under subsection (1) of this section may be  
26 recovered on behalf of class members only if the plaintiffs in the action  
27 establish that the members have sustained an ascertainable loss of money  
28 or property as a result of a reckless or knowing use or employment by the  
defendant of a method, act or practice declared unlawful by ORS 646.608;

(b) The trier of fact may award punitive damages; and

(c) The court may award appropriate equitable relief.

1 331. MGM engaged in a “reckless or knowing” use or employment of an unlawful trade  
2 practice for the reasons noted above regarding MGM’s unconscionable tactics.

3 332. As a direct and proximate result of MGM’s unfair and deceptive acts and practices,  
4 Plaintiff and the Oregon Subclass have suffered and will continue to suffer injury, ascertainable  
5 losses of money or property, and monetary and non-monetary damages, as alleged herein.

6 333. Plaintiff and the Oregon Subclass seek all monetary and non-monetary relief  
7 allowed by law, including actual damages, statutory damages, and punitive damages for MGM’s  
8 willful violations of the Oregon UTPA, as well as injunctive relief, attorneys’ fees, and all other  
9 relief available under Ore. Stat. §§ 646.636 and 646.638.

10 **COUNT XIV**  
11 **VIOLATION OF THE OREGON CONSUMER INFORMATION PROTECTION ACT**  
12 **Ore. Stat. §§ 646A.600, *et seq.***  
13 **(On Behalf of the Oregon Subclass)**

14 334. Plaintiff Dvorak (“Plaintiff” for purposes of this count) re-alleges and incorporates  
15 by reference all preceding allegations as if fully set forth herein.

16 335. The Oregon Consumer Information Protection Act (“Ore. CIPA”) states: “A  
17 covered entity . . . shall develop, implement and maintain *reasonable safeguards* to protect the  
18 security, confidentiality and integrity of personal information.” Ore. Stat. § 646A.622(1)  
(emphasis added).

19 336. The Ore. CIPA defines “covered entity” as a “person that owns, licenses, maintains,  
20 stores, manages, collects, processes, acquires or otherwise possesses personal information in the  
21 course of the person’s business.” Ore. Stat. § 646A.602(5)(a). MGM meets the definition of a  
22 covered entity.

23 337. The Ore. CIPA defines personal information as follows: “‘Personal information’  
24 means: (A) A consumer’s first name or first initial and last name in combination with any one or  
25 more of the following data elements: . . . (ii) A consumer’s driver license number or state  
26 identification card number issued by the Department of Transportation; [or] (iii) A consumer’s  
27 passport number or other identification number issued by the United States.” Ore. CIPA §  
28

1 646A.603(12)(a)(A). The PII stolen in the Data Breach includes personal information that meets  
2 this definition. Plaintiff Dvorak believes he presented his driver's license number to MGM when  
3 checking in for his MGM hotel stay, thus MGM possessed his driver's license number for purposes  
4 of this claim.

5 338. MGM failed to maintain reasonable safeguards to protect Plaintiff's and Oregon  
6 Subclass members' PII, for the reasons alleged herein. Accordingly, MGM violated Ore. Stat. §  
7 646A.622(1).

8 339. Pursuant to Or. Stat. § 646A.604(11), violations of Or. Rev. Stat. § 646A.622 are  
9 unlawful practices for purposes of the Oregon Unlawful Trade Practices Act, Or. Stat. § 646.607,  
10 as set forth in the preceding Count. Thus, MGM's violation of Or. Rev. Stat. § 646A.622(1) is an  
11 actionable act for purposes of Plaintiff's Oregon Unlawful Trade Practices Act claim.

12 340. Plaintiff and Oregon Subclass members were injured by MGM's violation of the  
13 Ore. CIPA. Plaintiff and the Oregon Subclass seek all monetary and non-monetary relief allowed  
14 by law to compensate for their various types of damages alleged herein.

15 **VII. REQUEST FOR RELIEF**

16 WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated,  
17 respectfully request the following relief:

- 18 (a) An Order certifying this case as a class action;
- 19 (b) An Order appointing Plaintiffs as class representatives;
- 20 (c) An Order appointing the undersigned counsel as class counsel;
- 21 (d) An award of compensatory damages, money for significant and reasonable  
22 identity protection services, statutory damages, treble damages, and punitive damages;
- 23 (e) Injunctive relief requiring MGM to: (i) strengthen its technical and  
24 administrative information security controls and adequately fund them for several years;  
25 (ii) submit to regular, independent SOC 2, Type 2 audits of its enterprise data networks and  
26 all security-relevant systems, with scoping and assertion statements established by an  
27 independent assessor; (iii) promptly implement all remediation measures recommended by  
28



1 the SOC 2, Type 2 assessor and any other forensic analysis or incident response entities  
2 retained to address the Data Breach; (iv) implement tokenization or column-level  
3 encryption of sensitive PII in all databases; (v) purge all PII that MGM no longer needs for  
4 processing Class members' prior hotel stays; and (vi) delete all PII from non-production  
5 database environments;

6 (f) An award of Plaintiffs' attorneys' fees and litigation costs; and

7 (g) Such other and further relief as this Court may deem just and proper.

8 **VIII. DEMAND FOR JURY TRIAL**

9 Plaintiffs demand a trial by jury as to all issues so triable.

10 Dated: April 2, 2021.

Respectfully submitted,

11 /s/ Don Springmeyer

12 Don Springmeyer (NBN 1021)

13 KEMP JONES, LLP

3800 Howard Hughes Parkway, 17th Floor

14 Las Vegas, NV 89169

Tel: (702) 385-6000

15 Email: d.springmeyer@kempjones.com

16 Miles N. Clark (NBN 13848)

17 Matthew I. Knepper (NBN 12579)

KNEPPER & CLARK LLC

5510 S. Fort Apache Rd., Suite 30

18 Las Vegas, NV 89148-7700

Tel: (702) 856-7430

19 Fax: (702) 447.8048

20 Email: miles.clark@knepperclark.com

Email: matthew.knepper@knepperclark.com

21 *Co-Liaison Counsel for Plaintiffs and the Class*

22 E. Michelle Drake (*Pro Hac Vice*)

23 BERGER MONTAGUE, PC

43 SE Main Street, Suite 505

24 Minneapolis, MN 55414

Tel: (612) 594-5933

25 Fax: (612) 584-4470

26 Email: emdrake@bm.net

-and-

27 Michael Dell'Angelo (*Pro Hac Vice*)

1 Jon Lambiras (*Pro Hac Vice*)  
2 Reginald Streater  
3 BERGER MONTAGUE, PC  
4 1818 Market Street, Suite 3600  
5 Philadelphia, PA 19103  
6 Tel: (215) 875-3000  
7 Fax: (215) 875-4604  
8 Email: mdellangelo@bm.net  
9 Email: jlambiras@bm.net  
10 Email: rstreater@bm.net

11 Douglas J. McNamara (*Pro Hac Vice*)  
12 Andrew N. Friedman (*Pro Hac Vice*)  
13 Geoffrey A. Graber (*Pro Hac Vice*)  
14 Paul Stephan (*Pro Hac Vice*)  
15 COHEN MILSTEIN SELLERS & TOLL, PLLC  
16 1100 New York Ave, 5th Floor  
17 Washington, DC 20005  
18 Tel: (202) 408-4600  
19 Fax: (202) 408-4699  
20 Email: dmcnamara@cohenmilstein.com  
21 Email: afriedman@cohenmilstein.com  
22 Email: ggraber@cohenmilstein.com  
23 Email: pstephan@cohenmilstein.com

24 David M. Berger (*Pro Hac Vice*)  
25 GIBBS LAW GROUP, LLP  
26 505 14th Street, Suite 110  
27 Oakland, CA 94612  
28 Tel: (510) 350-9700  
Fax: (510) 350-9701  
Email: dmb@classlawgroup.com

John A. Yanchunis (*Pro Hac Vice*)  
Jean S. Martin (*Pro Hac Vice*)  
Marcio Valladares (*Pro Hac Vice*)  
MORGAN & MORGAN  
COMPLEX LITIGATION GROUP  
201 N. Franklin Street, 7th Floor  
Tampa, FL 33602  
Tel: (813) 223-5505  
Fax: (813) 223-5402  
Email: jyanchunis@forthepeople.com  
Email: jeanmartin@forthepeople.com  
Email: mvalladares@forthepeople.com  
*Co-Lead Counsel for Plaintiffs and the Class*

**CERTIFICATE OF SERVICE**

I hereby certify that on April 2, 2021, a true and correct copy of the foregoing was served on all counsel of record via the Court's CM/ECF system.

By: /s/ Pamela Montgomery  
An employee of KEMP JONES, LLP

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28