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

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

Co-Liaison Counsel for Plaintiffs and the Class

(Additional Counsel Listed on Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

In re: MGM Resorts International Data Breach Litigation This Document Relates To: All Actions	Master Case No.: 2:20-cv-00376-GMN-NJK **CONSOLIDATED CLASS ACTION COMPLAINT**

TABLE OF CONTENTS

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

I. INTRODUCTION

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

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

3. PII stolen in the Data Breach has been posted to the "dark web" on at least three separate occasions, and continues to be extensively redistributed. MGM has acknowledged that the hacker "posted the data on a closed internet forum with the intent to sell the information for financial gain."[1]

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

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

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

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

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

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

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

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

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

II. PARTIES

A. Plaintiffs

1. California Plaintiffs

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

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

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

[2] The Identity Theft Resource Center has noted that email addresses stolen in the MGM Data Breach can be targets of emails embedded with ransomware. *See Information from MGM Data 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/ ("In order to get the recipient to click the link, the email just has to look like it came from MGM

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

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

---

Resorts – or another company the person does business with – and offer some plausible reason 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).

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

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

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

2. Connecticut Plaintiff

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

3. Georgia Plaintiff

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

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

4. Louisiana Plaintiff

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

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

5. New York Plaintiff

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

6. Ohio Plaintiff

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

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

7. Oregon Plaintiff

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

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

8. South Carolina Plaintiff

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

B. Defendant

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

in Prince George's County, Maryland; and MGM Springfield in Springfield, Massachusetts.[3] MGM's consolidated revenues and net income in 2019 were $13 billion and $2.2 billion, respectively.

III. JURISDICTION AND VENUE

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

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

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

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

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

---

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

[4] MGM's key data security employees are based at MGM's headquarters in Las Vegas. For 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, a review of MGM's information technology and data security job listings indicates that the vast majority of those positions are located in Las Vegas, including the "Vice President, Cyber Defense," "Director of Information Security Program Management," and "Executive Director,

IV. STATEMENT OF FACTS

A. The MGM Data Breach

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

28. MGM stated that it discovered the Data Breach three days later, on July 10, 2019.[5]

29. According to MGM, the hackers were able to obtain PII including customers' names, addresses, phone numbers, email addresses, and dates of birth. For some guests, the stolen data also included driver's license numbers, passport numbers, or military identification numbers.[6]

30. Cybersecurity journalists have recognized that the PII stolen in the Data Breach represents a "treasure trove" of "highly sensitive" personal information, and that affected consumers now face a risk of fraud and misuse of their PII.[7]

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

---

Identity Access Management." *See* https://careers.mgmresorts.com/global/en/c/technology-jobs (last visited Feb. 19, 2021).

[5] *See MGM Still Detangling Last Year's Data Breach*, June 8, 2020, *available at* 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 10, 2019, we learned that an unauthorized party had accessed and downloaded certain MGM Resorts guest data from an external cloud server a few days earlier.") (last visited Feb. 26, 2021).

[6] *See MGM Resorts Says Data Breach Exposed Some Guests' Personal Information*, The New York Times, Feb. 19, 2020, *available at* 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 Million Customers*, SC Magazine, Feb. 20, 2020, *available at* 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).

[7] *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-guests-posted-on-a-hacking-forum/ (last visited Feb. 26, 2021); *accord MGM Resorts Hack Exposes Details of 10.6 Million Guests*, Fortune, Feb. 20, 2020, *available at* https://fortune.com/2020/02/20/mgm-resorts-hack-data-breach-10-6-million-guests/ ("Identity theft is the big threat here.") (last visited Feb. 26, 2021).

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

> **Notice of Data Incident**
>
> **What Happened**
>
> On or about July 7, 2019, an individual accessed MGM Resorts International's computer network system without permission. **The individual downloaded partial customer data from MGM's computer systems, then posted and disclosed part of the data on a closed internet forum**. . . .
>
> **What Information Was Involved**
>
> MGM immediately initiated an internal forensic investigation into this incident. MGM conducted an exhaustive investigation and search of the downloaded data from the closed internet site. On August 9, 2019, **MGM determined your First Name, Last Name and Driver's License Number were part of the compromised file**. . . .
>
> **What We Are Doing**
>
> We take the security of our customers' data seriously, and after MGM became aware of the event, we took immediate measures to investigate and remediate the incident. We have implemented additional safeguards to improve further data security related to external software incidents. Furthermore, MGM reported the incident to law enforcement immediately once MGM discovered the matter. In addition, we are offering identity theft protection services through ID Experts, the data incident and recovery services expert, to provide you with MyIDCare. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.
>
> **What You Can Do**
>
> We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 833-959-1344 or going to https://ide.myidcare.com/mgmri and using the Enrollment Code provided above. . . .[8]

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

[8] *See* https://media.dojmt.gov/wp-content/uploads/Consumer-Notice-26.pdf (emphasis added) (last visited Feb. 26, 2021).

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

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

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

---

[9] *See* https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2019-09-09-MGM Resorts.pdf (emphasis added) (last visited Feb. 26, 2021).

[10] *Id*. (emphasis added).

[11] *See* https://media.dojmt.gov/wp-content/uploads/Consumer-Notice-26.pdf (last visited Feb. 26, 2021).

[12] *Id.*

[13] *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-guests-posted-on-a-hacking-forum/ (last visited Feb. 26, 2021); *accord MGM Admits to 2019 Data Breach Affecting 10.6 Million Customers*, SC Magazine, Feb. 20, 2020, *available at*

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

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

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

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

37. MGM has been unusually secretive about how the hackers were able to breach its systems and obtain consumers' PII. The scant information publicly released suggests that MGM is at fault. For example, an MGM spokesperson confirmed that the Data Breach resulted from "unauthorized access to a cloud server."[15] MGM's breach notification letters sent to Canadian residents corroborate this statement, noting that the hackers "downloaded . . . MGM Resorts guest

---

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).

[14] *See A Hacker is Selling Details of 142 Million MGM Hotel Guests on the Dark Web*, ZDNet, 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).

[15] *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-guests-posted-on-a-hacking-forum/ (quoting unnamed "MGM spokesperson") (last visited Feb. 26, 2021).

data from an external cloud server."[16] MGM also disclosed to the North Dakota Attorney General that the hackers "exfiltrated data by exploiting a compromised account."[17]

38. A data security professional noted that the breach "could have easily been caused from poor cloud configuration and security hygiene."[18]

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

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

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

> Sources sharing juicy tidbits about the MGM Resorts data hack we haven't seen elsewhere. Source believes hackers had ties to Iran. . . . About 52,000 people were notified, out of a reported 10.6 million.
>
> Per source, data was compromised via "SQL tables" posted "in the Cloud" within AWS (Amazon Web Services). Basically, "production data" stored in a development environment.
>
> * * *
>
> Source further explains, "due to data fields not being properly purged and tables improperly joined, those who used military I.D. and/or passport numbers had those numbers leaked along with their basic contact information." . . . .

---

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

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

[18] *See MGM Admits to 2019 Data Breach Affecting 10.6 Million Customers*, SC Magazine, Feb. 20, 2020, *available at* 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).

> Source says both the MGM Resorts player database (PATRON) and hotel database (OPERA) were compromised. Hackers leaked five million records to sell complete set of data, 200 million lines of data (one line of data per individual).
>
> Source also claims MGM Resorts paid hackers 'hundreds of thousands of dollars' to attempt to buy back the data, keep it from being released and to keep the data breach quiet. The data was leaked, anyway.[19]

42. The hackers stole the PII from MGM on July 7, 2019. MGM discovered the Data Breach on July 10, 2019.[20]

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

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

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

---

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

[20] *See MGM Still Detangling Last Year's Data Breach*, June 8, 2020, *available at* 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 10, 2019, we learned that an unauthorized party had accessed and downloaded certain MGM Resorts guest data from an external cloud server a few days earlier.") (last visited Feb. 26, 2021).

Consumer Reports has noted: "One thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. . . . If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves."[21]

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

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

47. MGM acknowledged that the first posting to the dark web took place on July 10, 2019, three days after the hackers accessed MGM's server.[22]

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

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

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

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

---

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

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

[23] *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-guests-posted-on-a-hacking-forum/ (last visited Feb. 26, 2021).

* * *

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

* * *

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

* * *

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

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

* * *

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

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

* * *

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

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

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

[24] *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-guests-posted-on-a-hacking-forum/ (emphasis added) (last visited Feb. 26, 2021).

> **details of 142,479,937 MGM hotel guests** . . . .
>
> * * *
>
> ZDNet . . . review[ed] two different batches of MGM data -- the 10.6 million user records leaked in February and a newer 20 million batch shared by the hackers on Sunday.
>
> Dates of birth and phone numbers were also included . . . .
>
> * * *
>
> Posts on Russian-speaking hacking forums promoted the MGM data breach as containing details on more than 200 million hotel guests.[25]

51. The stolen PII has been extensively redistributed after its initial postings to the dark web. Cybersecurity experts have stated that the PII was "shared on a popular hacking forum in February 2020 where it was **extensively redistributed**."[26]

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

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

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

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

[25] *See A Hacker is Selling Details of 142 Million MGM Hotel Guests on the Dark Web*, ZDNet, 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).

[26] *See* https://haveibeenpwned.com/PwnedWebsites (last visited Feb. 26, 2021) (emphasis added).

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

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

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

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

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

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

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

---

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

[28] *See MGM Admits to 2019 Data Breach Affecting 10.6 Million Customers*, SC Magazine, Feb. 20, 2020, *available at* 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).

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

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

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

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

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

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

exists here, *i.e.* a "risk . . . when [the PII] is combined with other available information to forge convincing phishing or identity fraud attacks."[29]

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

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

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

---

[29] *See New Details Indicate That Scope of the 2019 MGM Data Breach Is Much Bigger Than 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/ (last visited Feb. 26, 2021).

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

[31] *See* https://media.dojmt.gov/wp-content/uploads/Consumer-Notice-26.pdf ("Recommended Steps" attached to Notice) (last visited Feb. 26, 2021).

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

66. The Federal Trade Commission ("FTC") has promulgated various guides for businesses, which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[32]

67. In 2016, the FTC updated its publication titled *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[33] The guidelines stated that:

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

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

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

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

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

---

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

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

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

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

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

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

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

73. Similarly, the U.S. Government's National Institute of Standards and Technology (NIST) provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[35]

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

---

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

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

and incident response.[36] MGM failed to adhere to the NIST guidance.

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

a) Installing appropriate malware detection software;

b) Monitoring and limiting network ports;

c) Protecting web browsers and email management systems;

d) Setting up network systems such as firewalls, switches and routers;

e) Monitoring and protection of physical security systems; and

f) Training hotel staff regarding critical points.[37]

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

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

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

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

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

[36] *Id*. at Table 2 pg. 26-43.

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

noted that there were 338 breaches in the accommodation industry in 2017 alone, including at many of the major hotel brands.[39]

80. Trustwave's "2018 Global Security Report" listed hospitality as one of the top three industries targeted in payment card breaches.[40] Other estimates project that hotels are the targets of around 20% of all cyberattacks.[41]

81. In recent years, Choice Hotels, Hard Rock Hotel, Hilton, Hyatt, Kimpton, Marriott, Millennium, Omni, Radisson, Starwood, and Wyndham, among others, have all experienced data breach incidents.[42]

82. "Such unfortunate trends should not come as much of a surprise since hotels are hotbeds of sensitive information. Their data is spread out across porous digital systems . . . ."[43]

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

---

[38] *See Verizon 2018 Data Breach Investigations Report*, 11th Ed., at pp. 5, 25, 27, *available at* https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf (last visited Feb. 26, 2021).

[39] *Id.*

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

[41] *Id.*

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

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

cybercriminals much more value than breaching a company in almost any other industry."[44]

84. Notably, several prior hotel data breaches involved "exposed cloud servers," which is the same issue that reportedly led to the MGM breach.[45]

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

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

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

---

[44] *See Cybersecurity in Hospitality: An Unsolvable Problem?*, Paladion Networks, *available at* https://www.paladion.net/cybersecurity-in-hospitality-an-unsolvable-problem (last visited Feb. 26, 2021).

[45] *See MGM Admits to 2019 Data Breach Affecting 10.6 Million Customers*, SC Magazine, Feb. 20, 2020, *available at* 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).

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

[47] *See* https://s22.q4cdn.com/513010314/files/doc_downloads/committee/MGM-Audit-Committee-Charter-(FINAL).pdf (last visited Feb. 26, 2021).

G. MGM Uses Consumers' PII for Profit-Generating Purposes Beyond Processing Hotel Stays

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

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

> **Marketing Purposes**. We may use the information we collect for our own marketing purposes . . . .
>
> **Non-Marketing Purposes**. We may use the information we collect for non-marketing purposes including . . . (2) recording and accessing gaming-related activity . . . ; (3) conducting statistical or demographic analysis; . . . (6) customizing your experience while visiting . . . MGM Resorts; (7) protecting and defending MGM Resorts International and its affiliates against legal actions or claims; . . . [and] (9) collecting debt . . . .
>
> . . . . We may also link Personal Information with other generally or publicly available information to help us identify your preferences or interests. The information we collect may also be merged with information available from other sources such as (1) companies that match e-mail addresses with postal addresses and other information; . . . and (3) other subsidiaries, resorts, casinos, or properties that are owned, operated, or affiliated with MGM Resorts International.
>
> * * *
>
> **Sharing with Business Partners and Other Third Parties**. We may share the information we collect with our business partners and other third parties for joint marketing purposes or our business partners' (or our own) marketing purposes.[48]

90. MGM's self-serving motive to retain and mine its customers' PII led to MGM holding a massive trove of customer data for years after the customers' underlying hotel stays. 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

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

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

92. The FTC has long advised against this practice, stating: "If you don't have a legitimate business need for sensitive personally identifying information, don't keep it. In fact, don't even collect it. If you have a legitimate business need for the information, keep it only as long as it's necessary."[49]

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

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

H. Plaintiffs and Class Members Suffered Damages

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

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

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

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

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

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

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

1. Loss of Value of PII

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

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

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

[50] *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).

each.[51]

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

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

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

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

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

---

[51] *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).

[52] *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).

[53] *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).

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

108. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[54]

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

2. Benefit of Bargain Damages

110. Plaintiffs and Class members also suffered "benefit of bargain" damages.

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

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

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

[54] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets*, 15 Rich. J. L. & Tech. 11, 14 (2009).

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

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

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

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

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

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

(a) losing the inherent value of their PII;

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

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

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

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

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

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

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

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

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

I. Plaintiffs and Class Members are Entitled to Injunctive Relief

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

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

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

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

scoping and assertion statements established by an independent assessor;

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

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

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

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

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

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

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

V. CLASS ACTION ALLEGATIONS

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

---

[56] *See* https://www.upguard.com/security-report/mgmresorts (last visited March 2020).

[57] *See* https://www.upguard.com/security-report/mgmresorts (last visited Feb. 28, 2021).

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

NATIONWIDE CLASS

125. Plaintiffs seek certification of the following class:

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

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

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

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

STATEWIDE SUBCLASSES

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

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

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

> California Subclass: All residents of California whose PII was acquired by cybercriminals in the MGM Data Breach.
>
> Connecticut Subclass: All residents of Connecticut whose PII was acquired by cybercriminals in the MGM Data Breach.
>
> Georgia Subclass: All residents of Georgia whose PII was acquired by cybercriminals in the MGM Data Breach.

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

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

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

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

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

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

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

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

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

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

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

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

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

(f) Whether MGM's conduct constituted violations of state consumer protection statutes;

(g) Whether MGM's conduct constituted violations of state data security statutes;

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

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

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

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

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

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

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

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

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

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

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class)

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

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

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

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

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

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

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

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

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

circumstances would act; and

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

149. MGM was subject to an "independent duty," untethered to any express contract between MGM and Class members. The sources of MGM's independent duty are included in the list above.

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

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

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

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

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

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

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

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

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

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

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

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

COUNT II
NEGLIGENT MISREPRESENTATION
(On Behalf of the Nationwide Class)

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

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

> One who fails to disclose to another a fact that he knows may justifiably induce the other to act or refrain from acting in a business transaction is subject to the same 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

reasonable care to disclose the matter in question.

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

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

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

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

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

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

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

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

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

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

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

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

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

176. In addition to its omissions, MGM is also liable for its implied misrepresentations. 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 it employed reasonable data security practices to protect consumers' PII. By virtue of accepting Plaintiffs' PII during the reservation and check-in process, MGM implicitly represented that its data security processes were sufficient to reasonably safeguard the PII. This constituted a negligent misrepresentation.

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

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

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

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

193. Plaintiffs and Class members conferred benefits upon MGM.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

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

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.

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

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.

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

(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.

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

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

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

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

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

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

(b) MGM also made implied or implicit false representations that its data security practices 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 virtue of accepting Plaintiffs' PII during the reservation and check-in process, MGM implicitly represented that its data security procedures were sufficient to safeguard the PII. Those representations were false and misleading.

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

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

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

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

(b) MGM also made implied or implicit false representations that its data security practices 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 virtue of accepting Plaintiffs' PII during the reservation and check-in process, MGM implicitly represented that its data security processes were sufficient to safeguard the PII. Those representations were unfair, deceptive, untrue, or misleading.

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

in California by, among other things, making hotel reservations from California and paying any necessary room deposits from California. MGM acknowledges that "Southern California [is] where a large number of our customers reside."[58] The California Plaintiffs and California Subclass members were deceived in California when they made reservations from California and were not informed of MGM's deficient data security practices.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

241. Cal. Civ. Code § 1770(a) states:

> (a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction . . . that results in the sale or lease of goods or services to any consumer are unlawful:
>
> . . . .
>
> (5) Representing that goods or services have . . . characteristics, . . . uses,

> [or] benefits . . . that they do not have . . . [or]
>
> . . . .
>
> (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.

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

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

244. MGM's unlawful acts included the following:

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

(b) MGM also made implied or implicit representations that its data security practices 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 virtue of accepting Plaintiffs' PII during the reservation and check-in process, MGM implicitly represented that its data security processes were sufficient to safeguard the PII. Those representations were false and misleading.

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

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

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

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

248. Cal. Civ. Code § 1780(a) states:

> Any consumer who suffers any damage as a result of the use or employment by any 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:
>
> (1) Actual damages, but in no case shall the total award of damages in a class action be less than one thousand dollars ($1,000).
>
> (2) An order enjoining the methods, acts, or practices.
>
> (3) Restitution of property.
>
> (4) Punitive damages.
>
> (5) Any other relief that the court deems proper.

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

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

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

unlawful methods, acts, or practices.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

263. The CCRA defines personal information as follows: "'Personal information' means

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

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

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

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

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

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

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

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

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

(a) Failing to adopt reasonable data security procedures to adequately safeguard consumers' PII;

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

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

(d) Making implied or implicit representations that its data security practices 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 virtue of accepting Plaintiffs' PII during the reservation and check-in process, MGM implicitly represented that its data security processes were sufficient to safeguard the PII; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

286. 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

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

(b) Making implied or implicit representations that its data security practices 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 virtue of accepting Plaintiffs' PII during the reservation and check-in process, MGM implicitly represented that its data security processes were sufficient to safeguard the PII.

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

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

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

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

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

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

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

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

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

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

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

(b) Making implied or implicit representations that its data security practices 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 virtue of accepting Plaintiffs' PII during the reservation and check-in process, MGM

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

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

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

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

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

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

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

> [A]ny person who has been injured by reason of any violation of this section may bring an action in his own name to enjoin such unlawful act or practice, an action to recover his actual damages or fifty dollars, whichever is greater, or both such actions. The court may, in its discretion, increase the award of damages to an 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) Making implied or implicit representations that its data security practices 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 virtue of accepting Plaintiffs' PII during the reservation and check-in process, MGM implicitly represented that its data security processes were sufficient to safeguard the PII; and

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

Act, 15 U.S.C. § 45.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) Making implied or implicit representations that its data security practices 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

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

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

(d) Failing to implement reasonable data security measures to protect consumers' PII; and

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

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

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

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

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

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

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

325. Ore. Stat. § 646.638(1) states:

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

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

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

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

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

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

> A class action may be maintained under this section. In any class action under this section:
>
> (a) Statutory damages under subsection (1) of this section may be recovered on behalf of class members only if the plaintiffs in the action establish that the members have sustained an ascertainable loss of money 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.

331. MGM engaged in a "reckless or knowing" use or employment of an unlawful trade practice for the reasons noted above regarding MGM's unconscionable tactics.

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

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

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

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

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

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

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

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

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

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

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

VII. REQUEST FOR RELIEF

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

(a) An Order certifying this case as a class action;

(b) An Order appointing Plaintiffs as class representatives;

(c) An Order appointing the undersigned counsel as class counsel;

(d) An award of compensatory damages, money for significant and reasonable identity protection services, statutory damages, treble damages, and punitive damages;

(e) Injunctive relief requiring MGM to: (i) strengthen its technical and administrative information security controls and adequately fund them for several years; (ii) submit to regular, independent SOC 2, Type 2 audits of its enterprise data networks and all security-relevant systems, with scoping and assertion statements established by an independent assessor; (iii) promptly implement all remediation measures recommended by

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

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

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

VIII. DEMAND FOR JURY TRIAL

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

Dated: April 2, 2021.

Respectfully submitted,

/s/ Don Springmeyer

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

Miles N. Clark (NBN 13848)
Matthew I. Knepper (NBN 12579)
KNEPPER & CLARK LLC
5510 S. Fort Apache Rd., Suite 30
Las Vegas, NV 89148-7700
Tel: (702) 856-7430
Fax: (702) 447.8048
Email: miles.clark@knepperclark.com
Email: matthew.knepper@knepperclark.com
Co-Liaison Counsel for Plaintiffs and the Class

E. Michelle Drake (*Pro Hac Vice*)
BERGER MONTAGUE, PC
43 SE Main Street, Suite 505
Minneapolis, MN 55414
Tel: (612) 594-5933
Fax: (612) 584-4470
Email: emdrake@bm.net
-and-

Michael Dell'Angelo (*Pro Hac Vice*)

Jon Lambiras (*Pro Hac Vice*)
Reginald Streater
BERGER MONTAGUE, PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4604
Email: mdellangelo@bm.net
Email: jlambiras@bm.net
Email: rstreater@bm.net

Douglas J. McNamara (*Pro Hac Vice*)
Andrew N. Friedman (*Pro Hac Vice*)
Geoffrey A. Graber (*Pro Hac Vice*)
Paul Stephan (*Pro Hac Vice*)
COHEN MILSTEIN SELLERS & TOLL, PLLC
1100 New York Ave, 5th Floor
Washington, DC 20005
Tel: (202) 408-4600
Fax: (202) 408-4699
Email: dmcnamara@cohenmilstein.com
Email: afriedman@cohenmilstein.com
Email: ggraber@cohenmilstein.com
Email: pstephan@cohenmilstein.com

David M. Berger (*Pro Hac Vice*)
GIBBS LAW GROUP, LLP
505 14th Street, Suite 110
Oakland, CA 94612
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