DON SPRINGMEYER, ESQ. (SBN 1021)
DANIEL BRAVO, ESQ. (SBN 13078)
A. JILL GUINGCANGCO, ESQ. (SBN 14717)
WOLF, RIFKIN, SHAPIRO, SCHULMAN & RABKIN, LLP
3556 E. Russell Road, 2nd Floor
Las Vegas, Nevada 89120
Telephone: (702) 341-5200 / Fax: (702) 341-5300
Email: dspringmeyer@wrslawyers.com
Email: dbravo@wrslawyers.com
Email: ajg@wrslawyers.com

BERGER MONTAGUE PC
Michael Dell'Angelo (*Pro Hac Vice to be submitted*)
Jon Lambiras (*Pro Hac Vice to be submitted*)
Joshua T. Ripley (*Pro Hac Vice to be submitted*)
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000 / Fax: (215) 875-4604
mdellangelo@bm.net
jlambiras@bm.net
jripley@bm.net

Attorneys for Plaintiffs
(Additional Attorneys listed below)

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

LARRY LAWTER, JULIE MUTSKO, KERRI SHAPIRO, and VICTOR WUKOVITS, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

MGM RESORTS INTERNATIONAL,

Defendants.

Case No.: 20cv529

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiffs Larry Lawter, Julie Mutsko, Kerri Shapiro, 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 on behalf of millions of consumers whose

sensitive personal information was stolen by cybercriminals in a massive cyber-attack at MGM.

2. MGM is a global company that owns, operates, and manages hotels, casinos, and resorts, including in Las Vegas, Nevada.

3. On February 19, 2020, MGM publicly acknowledged that on July 7, 2019, an unauthorized individual gained access to MGM's computer systems and stole highly sensitive personally identifiable information ("PII") associated with more than 10.6 million hotel guests (the "Data Breach").

4. The stolen PII included names, addresses, phone numbers, email addresses, and dates of birth for guests who stayed at an MGM property through 2019. For certain guests, the stolen data also included driver's license numbers, passport numbers, or military identification numbers.

5. The stolen PII has been made available for download on the dark web, where it was posted to a popular hacking forum. Technology journalists at ZDNet and security researchers from Under the Breach were able to validate the origin of the posted data by using the PII to contact users and confirm that they stayed at an MGM property prior to the breach.

6. After being alerted of these findings, MGM belatedly confirmed that the data released on the dark web was obtained in the Data Breach.

7. The Data Breach was a direct result of MGM's failure to implement adequate and reasonable cyber-security procedures necessary to protect its customers' PII.

8. MGM disregarded the rights of Plaintiffs and class members by, among other things, failing to take adequate and reasonable measures to ensure that its data systems were protected against unauthorized intrusions; misrepresenting in its Privacy Policy that it had adequate data security practices in place to safeguard customers' PII; failing to take standard and readily available steps to prevent the data intrusion; and failing to monitor and timely detect the Data Breach.

9. Plaintiffs were guests at various MGM hotels during the period covered by the Data Breach. In connection with their reservations, Plaintiffs were required to provide MGM

with PII of the type included in the breach.

10. Plaintiffs and class members have sustained compensable damages as a result of the Data Breach. They have been exposed to a heightened and imminent risk of fraud and identity theft. They must now and indefinitely in the future closely monitor their financial accounts and credit reports to guard against fraud. This is a time-consuming process. They are also faced with undertaking costly measures to mitigate the impact of the breach. For example, to guard against identity theft, many class members will place credit freezes or fraud alerts on their credit reports, purchase credit monitoring or other identity protection services, or pay for credit reports. They will also investigate and dispute fraudulent activity incurred in their names. Plaintiffs and class members also suffered "benefit of the bargain" damages in that they paid money to MGM for services they would not have purchased, or would not have paid the same price for, had they known that MGM lacked adequate data security practices. Further, Plaintiffs and class members suffered a loss of value of their PII as a result of the breach.

11. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was stolen in the Data Breach. Plaintiffs seek remedies including reimbursement of fraud losses and other out-of-pocket costs; compensation for time spent in response to the Data Breach; free credit monitoring and identity theft insurance beyond MGM's current one-year offer; and injunctive relief involving substantial improvements to MGM's data security systems.

II. PARTIES

12. Plaintiff Larry Lawter is a resident of South Carolina. He paid for a hotel room at an MGM property during the relevant period, including but not limited to at the MGM Grand in May 2017. In connection with his hotel stay, he provided MGM with PII of the type at issue in the Data Breach. Plaintiff Lawter values the importance of data security and the privacy of his PII. Had he known the truth about MGM's deficient data security practices, he would not have stayed at an MGM property, or would not have paid the price that he paid. In response to the Data Breach, Plaintiff Lawter has spent time monitoring his financial accounts more closely than

he otherwise would.

13. Plaintiff Julie Mutsko is a resident of Ohio. She paid for a hotel room at MGM properties during the relevant period, including but not limited to at Monte Carlo in May 2015; at Mandalay Bay in May 2016; and at MGM Grand in May 2019. In connection with her hotel stays, she provided MGM with PII of the type at issue in the Data Breach. Plaintiff Mutsko values the importance of data security and the privacy of her PII. Had she known the truth about MGM's deficient data security practices, she would not have stayed at MGM properties, or would not have paid the price that she paid. In response to the Data Breach, Plaintiff Mutsko has spent time monitoring her financial accounts more closely than she otherwise would.

14. Plaintiff Kerri Shapiro is a resident of New York. She paid for a hotel room at MGM properties during the relevant period, including but not limited to at Bellagio in July 2016 and at Aria in July 2017. In connection with her hotel stays, she provided MGM with PII of the type at issue in the Data Breach. Plaintiff Shapiro values the importance of data security and the privacy of her PII. Had she known the truth about MGM's deficient data security practices, she would not have stayed at MGM properties, or would not have paid the price that she paid. In response to the Data Breach, Plaintiff Shapiro has spent time monitoring her financial accounts more closely than she otherwise would.

15. Plaintiff Victor Wukovits is a resident of Louisiana. He paid for a hotel room at an MGM property during the relevant period, including but not limited to at Luxor in February 2017. In connection with his hotel stay, he provided MGM with PII of the type at issue in the Data Breach. Plaintiff Wukovits values the importance of data security and the privacy of his PII. Had he known the truth about MGM's deficient data security practices, he would not have stayed at an MGM property, or would not have paid the price that he paid. In response to the Data Breach, Plaintiff Wukovits has spent time monitoring his financial accounts more closely than he otherwise would.

16. Defendant MGM Resorts International is a publicly traded company incorporated in Delaware. Its headquarters are located at 3600 Las Vegas Boulevard South, Las Vegas, NV

89109. It is a global hospitality and entertainment company. MGM's portfolio of hotels includes Aria, Bellagio, MGM Grand, Mandalay Bay, The Mirage, Luxor, New York-New York, Excalibur, Park MGM, and Circus Circus, among others. MGM earned consolidated net income of $2.2 billion in 2019.

III. JURISDICTION AND VENUE

17. 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 $5,000,000.00 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.

18. This Court has diversity jurisdiction over Plaintiffs' claims pursuant to 29 U.S.C. § 1332, as the parties are completely diverse and the amount in controversy exceeds $75,000.00.

19. This Court has general personal jurisdiction over MGM because it maintains its principal place of business in this District. The Court also has specific personal jurisdiction over MGM because it purposefully availed itself of this forum by engaging in suit-related conduct here, including the collection and storage of PII from Plaintiffs and class members.

20. 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, maintains customer PII in this District, and entered into consumer transactions with Plaintiffs and class members in this District.

IV. STATEMENT OF FACTS

A. The MGM Data Breach

21. On or about July 7, 2019, an unauthorized individual gained access to MGM's computer network and stole customer data for 10.6 million MGM customers.

22. The data consisted of a treasure trove of MGM customers' PII, including their 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.[1]

23. In mid-February 2020, the stolen data of all 10.6 million MGM guests was published on a well-known hacking forum used for buying and selling stolen PII, accessible to any number of "dark web" miscreants.

24. Cyber security specialists have recognized that the PII stolen in the Data Breach presents a "treasure trove" of "highly sensitive" personal information, and that many of the affected consumers now "face a higher risk" of misuse of the PII.[2]

25. On or about September 7, 2019, MGM began notifying affected customers and various governmental agencies of the Data Breach, although the notifications were not yet made public. MGM sent a Notice of Data Incident ("Notice") to affected customers and Attorneys General of various states. An example of one of the Notices 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

[1] *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.

[2] *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/.

> 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. . . .
>
> . . . .
>
> Please call 833-959-1344 or go to https://ide.myidcare.com/mgmri for assistance or for any additional questions you may have.[3]

26. In a letter to the North Dakota Attorney General dated September 7, 2019, MGM noted that the hacker "exfiltrated data by exploiting a compromised account concerning a third-party integration."[4] The letter also stated that **the hacker "posted the data on a closed internet forum with the intent to sell the information for financial gain**."[5]

27. MGM acknowledged that consumers face a substantial risk of fraud and identity theft from the Data Breach. The Notice contained an attachment with several "Recommended Steps" for consumers. It encouraged consumers to: (i) "Review your credit reports," (ii) "Place fraud alerts with the three credit bureaus," and (iii) place a "Security Freeze" on their credit files.[6] It also encouraged consumers to sign up for MGM's free credit monitoring offer. These steps illustrate the very real risks faced by consumers, and the protective measures needed to

---

[3] https://media.dojmt.gov/wp-content/uploads/Consumer-Notice-26.pdf (emphasis added).

[4] https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2019-09-09-MGMResorts.pdf.

[5] *Id.*

[6] https://media.dojmt.gov/wp-content/uploads/Consumer-Notice-26.pdf (attachment to Notice).

mitigate those risks.

28. In mid-February 2020, the stolen data of all 10.6 million MGM guests was published on a hacking forum used for buying and selling stolen PII. An article by data security researchers at ZDNet dated February 19, 2020 stated the following:

> **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.**
>
> . . . .
>
> 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 2019].**
>
> . . . .
>
> According to Irina Nesterovsky, Head of Research at threat intel firm KELA, the data of MGM Resorts hotel guests had been shared in some [other] closed-circle hacking forums since at least July, last year.
>
> . . . .
>
> [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.[7]

29. These facts illustrate that class members face a significant risk of identity theft or other misuse of their PII. Cyber-criminals would not buy and sell class members' PII unless they

[7] *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).

intended to misuse use it.

30. The Data Breach was reportedly the result of a faulty cloud-based server. A data security professional noted that the breach "could have easily been caused from poor cloud configuration and security hygiene."[8]

31. MGM is a multi-billion-dollar company and had the financial and personnel resources necessary to prevent the breach. MGM nevertheless neglected to adequately invest in reasonable data security measures.

32. As a condition of staying at its hotel properties, MGM requires that its customers entrust it with highly sensitive PII. By obtaining, collecting, using, and deriving a benefit from consumers' PII, MGM assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII. MGM failed to adopt reasonable safeguards despite its known duties.

B. MGM's Privacy Policy

33. MGM's Privacy Policy on its website discussed its data security safeguards and made materially false and misleading representations. The Privacy Policy stated the following, in relevant part:

MGM RESORTS PRIVACY POLICY

> MGM . . . respects your privacy. This Privacy Policy ("Policy") describes the information collection, use, protection, and sharing practices of MGM Resorts International and MGM Resorts International websites, mobile applications, electronic communications, and properties.
>
> We collect information from a variety of sources and in a variety of ways, including the following:
>
> **Personal Information**. When you visit, use, and/or access MGM Resorts or MGM Online Services, you may provide us with (and/or we may collect) information by which you can be personally identified including your name, date of birth, postal address, email address, and telephone number, and videos, recordings, and images of you ("Personal Information"). We may also obtain Personal Information from third parties.

[8] *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/.

> **Sensitive Information.** When you make a purchase, visit, use and/or access MGM Resorts or MGM Online Services, or engage in other transactions or activities, you may provide us with sensitive Personal Information including your credit or debit card number, financial account number, biometrics, medical/health-related information, driver's license number, government-issued identification card number, social security number, passport number, or naturalization number ("Sensitive Information").
>
> **SECURITY**
>
> Information maintained in electronic form that is collected by MGM Resorts International and any individual MGM Resort is stored on systems **protected by industry standard security measures**. These measures are intended to **protect these systems from unauthorized access. . . . We have controls in place that are designed to detect potential data breaches, contain and minimize the loss of data**, and conduct forensic investigations of a breach.
>
> **Our staff is required to take reasonable measures to ensure that unauthorized persons cannot view or access your Personal Information.** Employees who violate our internal privacy policies are subject to disciplinary action up to and including termination of employment.[9]

34. These representations were false and misleading because, among other things, MGM did not employ "industry standard security measures," did not have controls in place to "detect potential data breaches," and did not take "reasonable measures to ensure that unauthorized persons cannot view or access your Personal Information." The Privacy Policy also contained material omissions because it failed to disclose the shortfalls in MGM's data security practices.

35. Plaintiffs and class members provided their PII to MGM with the reasonable expectation and mutual understanding that MGM would comply with its obligations to keep the PII confidential and would take reasonable steps to secure it from theft. MGM failed to do so, in violation of its own Privacy Policy.

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

36. The type of PII collected by hotels makes this industry particularly appealing to

[9] https://www.mgmresorts.com/en/privacy-policy.html (emphasis added).

cyber criminals. Trustwave's "2018 Global Security Report" listed hospitality as one of the top three industries most vulnerable to payment card breaches.[10] Other estimates project that hotels are the targets of around 20% of all cyberattacks.[11]

37. Indeed, in recent years, Marriott, Hilton, Hyatt, and Trump Hotels have all been cited for large-scale data negligence. "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 and their sales are usually conducted through weak point-of-sale systems."[12]

38. "Hotel chains and travel companies were major targets for cybercriminals in 2019 with several being hit with . . . card skimming malware and others suffering from exposed cloud servers . . . ."[13]

39. "While hospitality companies have fewer transactions than retail organizations — and thus have data on fewer customers to steal – they collect substantially more valuable and varied personal data for each of their guests. . . . This rich personal data is invaluable to cybercriminals. They can use this data to better impersonate each breached customer, leading to additional identity theft and social engineering attacks against each individual's company. By enabling further attacks, breaching a hotel provides cybercriminals much more value than breaching a company in almost any other industry."[14]

40. The increased risk of data breaches in the hotel industry was widely known throughout the hospitality field, including to MGM. MGM knew or should have known of the

---

[10] *Why Cybersecurity Matters*, Hotel Management (Oct. 17, 2019), *available at* https://www.hotelmanagement.net/tech/why-cybersecurity-matters.

[11] *Id.*

[12] *Id.*

[13] *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/.

[14] *Cybersecurity in Hospitality: An Unsolvable Problem?*, Paladion Networks, *available at* https://www.paladion.net/cybersecurity-in-hospitality-an-unsolvable-problem.

substantial and foreseeable risk of a data breach involving the PII it held. Despite the known risks, MGM failed to adopt commercially reasonable and readily available safeguards.

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

D. The Risk of Misuse of the Stolen PII Will Persist for Years

42. MGM was well aware that the PII it collects is highly sensitive, and of significant value to those who would wish to use it for wrongful purposes.

43. PII is a valuable commodity to identity thieves. As the Federal Trade Commission ("FTC") recognizes, with stolen PII identity thieves can commit an array of crimes including identify theft and financial fraud.[15]

44. A robust cyber black market exists, in which criminals can post stolen PII on multiple underground websites. That is exactly what took place here.

45. The ramifications of MGM's failure to keep PII secure are long lasting. Once PII is stolen, fraudulent use of that information, and re-sale among cyber criminals, may continue for years.

46. "The fact that the breach happened about seven months ago without any public disclosure may have led MGM to believe the data was not going to be used by the thieves, but as 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. It's likely MGM thought this incident was far in the rear view, but the value of their particular dataset continues to have appeal."[16]

47. Thus, even if misuse has not yet occurred for certain class members, there is a substantial risk that misuse will take place in the future. Accordingly, class members must

---

[15] *Warning Signs of Identity Theft*, Federal Trade Commission, *available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

[16] *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/.

remain vigilant and closely monitor their financial affairs indefinitely. MGM's offer of free credit monitoring for just one year is inadequate.

E. MGM Failed to Comply with FTC Guidelines and Industry Standards

48. The FTC has promulgated numerous 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.[17]

49. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[18] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone is attempting to gain unauthorized access to the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

50. The FTC further recommends 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.[19]

51. The FTC has brought enforcement actions against businesses for failing to

---

[17] *Start With Security*, Federal Trade Commission, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[18] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[19] *Start With Security*, Federal Trade Commission, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

adequately protect customer data, treating the failure to employ reasonable safeguards as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

52. MGM failed to adopt reasonable data security safeguards. MGM's failure to protect customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

53. Cyber security firms and industry participants have promulgated a series of best practices that should be implemented by hospitality companies, including but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training hotel staff regarding critical points.[20]

54. MGM failed to comply with these and other industry best practices.

F. Plaintiffs and Class Members Suffered Damages

55. As a direct and proximate result of MGM's wrongful actions and inactions, Plaintiffs and class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud. The increased risk requires them to spend time and money to mitigate the actual and potential impacts of the Data Breach.

56. Plaintiffs and class members have suffered, will suffer, or are at a substantially increased risk of suffering the following types of harm, among others:

a. The unauthorized use of their PII for fraudulent purposes.

b. Fraud losses for accounts opened or debts incurred in their name.

c. Out-of-pocket costs for mitigation efforts such as purchasing credit

[20] *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/.

monitoring services, credit freezes, credit reports, etc.

d. Time spent responding to the Data Breach for things like reviewing financial accounts and credit reports more closely than they otherwise would have, researching and disputing fraudulent charges or suspicious activity, signing up for protective measures, etc.

e. Lost opportunity costs and lost wages associated with efforts expended in response to the Data Breach.

f. "Loss of value" of their PII. A robust market exists for stolen PII, which is highly coveted and sold on the dark web at specific identifiable prices. The theft of consumers' PII led to a diminution in value of that PII.

g. "Benefit of the bargain" damages. Plaintiffs and class members overpaid for hotel services that should have been – but were not – accompanied by adequate data security. Part of the price class members paid to MGM was intended to be used to fund adequate data security. Plaintiffs and class members did not get what they paid for. MGM's misrepresentations and omissions regarding data security diminished the value of Plaintiffs' purchases.

h. The continued risk to their PII in MGM's possession, which could be the subject to further breaches if MGM fails to undertake appropriate measures to protect the PII going forward.

57. Consumers face an unusually high risk of misuse from this particular data breach. Criminals stole the PII with the specific intent to use it for fraudulent purposes and/or to sell it to others for purposes of misusing it. The PII has already been posted on the dark web, and it is only a matter of time before it is misused on a large scale.

58. Identity thieves can combine data stolen in the Data Breach with other information about class members gathered from underground sources, public sources, or even class members' social media accounts.

59. Thieves can also use the stolen data, alone or in combination with other information about the individual, to send highly targeted phishing emails to class members to obtain more sensitive information.

60. Thieves can use the stolen data, alone or in combination with other information about the individual, to commit crimes including, *e.g.*, opening new financial accounts in class members' names; taking out loans in class members' names; using class members' information to obtain government benefits; filing fraudulent tax returns using class members' information; obtaining driver's licenses in class members' names but with another person's photograph; and giving false information to police during an arrest.

61. MGM has acknowledged that consumers face a significant risk of identity theft or other misuse stemming from the Data Breach. As noted above, MGM recommended that affected consumers: (i) "Review your credit reports," (ii) "Place fraud alerts with the three credit bureaus," and (iii) place a "Security Freeze" on their credit files.[21] Those steps would not be necessary if the risk of harm was *de minimis*.

G. MGM's Delay in Providing Notice to Class Members Caused Additional Harm

62. "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."[22]

63. Consumers' PII was stolen on July 7, 2019, but MGM did not begin to send notice to affected customers until September 2019, depriving them of the ability to promptly mitigate potential adverse consequences of the Data Breach.

---

[21] https://media.dojmt.gov/wp-content/uploads/Consumer-Notice-26.pdf (attachment to sample Notice).

[22] *The Data Breach Next Door*, Consumer Reports, Jan. 31, 2019, *available at* https://www.consumerreports.org/data-theft/the-data-breach-next-door/.

64. As a result of MGM's unreasonable delay in detecting and notifying consumers of the Data Breach, the risk of harm to Plaintiffs and class members has been increased.

H. Plaintiffs and Class Members Are Entitled to Injunctive Relief

65. Plaintiffs and class members are entitled to injunctive relief requiring MGM to, among other things: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all class members.

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

V. CLASS ACTION ALLEGATIONS

67. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of a Nationwide Class. In the alternative, Plaintiffs bring this case on behalf of the following state-specific subclasses: a Nevada Sub-Class, a Louisiana Sub-Class, a New York Sub-Class, an Ohio Sub-Class, and a South Carolina Sub-Class, defined as follows:

> Nationwide Class: All persons residing in the United States whose PII was stolen in the July 7, 2019 Data Breach at MGM.
>
> Nevada Sub-Class: All residents of Nevada whose PII was stolen in the July 7, 2019 Data Breach at MGM.
>
> Louisiana Sub-Class: All residents of Louisiana whose PII was stolen in the July 7, 2019 Data Breach at MGM.
>
> New York Sub-Class: All residents of New York whose PII was stolen in the July 7, 2019 Data Breach at MGM.
>
> Ohio Sub-Class: All residents of Ohio whose PII was stolen in the July 7, 2019 Data Breach at MGM.
>
> South Carolina Sub-Class: All residents of South Carolina whose PII was stolen in the July 7, 2019 Data Breach at MGM.

68. Excluded from the Classes are Defendant's executive officers, and the judge to

whom this case is assigned.

69. Plaintiffs hereby reserve the right to amend or modify these class definitions after having an opportunity to conduct discovery.

70. Numerosity. The Classes are each so numerous that joinder of all members is impracticable. The Nationwide Class consists of 10.6 million individuals, and the state Sub-Classes each consist of thousands or more individuals.

71. Commonality. There are many questions of law and/or fact common to Plaintiffs and the Classes. Common questions include, but are not limited to, the following:

a. Whether MGM's data security systems prior to the Data Breach complied with applicable data security laws, regulations, and industry standards;

b. Whether MGM owed a duty to class members to safeguard their PII;

c. Whether MGM breached its duty to class members to safeguard their PII;

d. Whether a computer hacker stole class members' PII in the Data Breach;

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

f. Whether Plaintiffs and class members suffered legally cognizable damages as a result of the Data Breach; and

g. Whether Plaintiffs and class members are entitled to injunctive relief.

72. Typicality. Plaintiffs' claims are typical of the claims of all class members because Plaintiffs, like all other class members, suffered a theft of their PII in the Data Breach.

73. Adequacy of Representation. Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs have retained competent and capable counsel with significant experience in complex class action litigation, including data breach class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Classes. Plaintiffs' counsel has the financial and personnel resources to do so. Neither Plaintiffs nor their counsel have any interests that are contrary to, or that conflict with, those of the Classes.

74. Predominance. MGM has engaged in a common course of conduct toward all

class members. The common issues arising from MGM's conduct predominate over any issues affecting just individual class members. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

75. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would find that the cost of litigating their individual claim is prohibitively high, and they would have no effective remedy on an individual non-class basis. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to class members, which would establish incompatible standards of conduct for MGM. In contrast, conducting this action on a class-wide basis presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of all class members.

76. MGM acted on grounds that apply generally to the Classes as a whole, so that injunctive relief is appropriate on a class-wide basis pursuant to Fed. R. Civ. P. 23(b)(2).

77. Likewise, particular "issues" under Rule 23(c)(4) are appropriate for certification because such matters present particular common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to, those included in the bulleted list above.

78. Finally, all members of the proposed Classes are readily ascertainable. MGM has access to customer names and addresses affected by the Data Breach. Using this information, class members can be identified and ascertained for the purpose of providing notice.

VI. CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On Behalf of the Nationwide Class and all State Sub-Classes)

79. Plaintiffs re-allege and incorporate by reference all preceding allegations as if

fully set forth herein.

80. As a condition of receiving services, Plaintiffs and class members were obligated to provide MGM with their PII.

81. Plaintiffs and class members entrusted their PII to MGM with the understanding that MGM would safeguard their PII.

82. MGM had knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and class members could suffer if the PII was stolen in a data breach.

83. MGM had a duty to exercise reasonable care in safeguarding, securing, and protecting such PII. This duty includes, among other things, designing, maintaining, and testing MGM's security protocols to ensure that PII was adequately secured and protected, and that employees tasked with maintaining such PII were adequately trained on cyber security measures.

84. MGM's duty of care arose as a result of, among other things, the special relationship that existed between MGM and its customers. MGM was in position to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur, which would result in substantial harm to consumers.

85. Also, MGM had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to use reasonable measures to protect confidential consumer data.

86. MGM was also subject to an "independent duty" untethered to any contract between class members and MGM.

87. Plaintiffs and class members were the foreseeable victims of inadequate data security practices and the theft of PII.

88. MGM knew or should have known of the inherent risks in collecting and storing PII, the critical importance of providing adequate security of that PII, and the frequent cyber-crimes being perpetrated in the hotel industry.

89. MGM's conduct created a foreseeable risk of harm to Plaintiffs and class

members. MGM's misconduct included, but was not limited to, its failure to take appropriate steps to prevent the Data Breach as set forth herein. MGM's misconduct also included its decision not to comply with industry standards for the safekeeping of PII.

90. Plaintiffs and class members had no ability to protect their PII once in was in MGM's possession.

91. MGM was in a position to protect against the harm suffered by Plaintiffs and class members as a result of the Data Breach.

92. MGM, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and class members by failing to exercise reasonable care in protecting and safeguarding PII while it was within the MGM's possession or control.

93. MGM improperly and inadequately safeguarded Plaintiffs' and class members' PII in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

94. But for MGM's wrongful breach of duties owed to Plaintiffs and class members, their PII would not have been stolen by computer hackers.

95. There is a temporal and close causal connection between MGM's failure to implement adequate security measures to protect PII and the harm suffered by Plaintiffs and class members.

96. As a result of MGM's negligence, Plaintiffs and class members suffered and will continue to suffer damages and injury set forth above.

97. Plaintiffs and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

98. Plaintiffs and class members are also entitled to the injunctive relief set forth above.

COUNT II

NEGLIGENCE *PER SE*

(On Behalf of the Nationwide Class and all State Sub-Classes)

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

100. Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of MGM's duty in this regard.

101. MGM violated Section 5 of the FTCA by failing to use reasonable measures to protect customer PII and not complying with applicable industry standards, as described in detail herein. MGM's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and class members.

102. MGM's violation of Section 5 of the FTCA constitutes negligence *per se* as MGM's violation of the FTCA establishes the duty and breach elements of negligence.

103. Plaintiffs and class members are within the class of persons that the FTCA was intended to protect.

104. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures, caused the same types of harm as those suffered by Plaintiffs and class members.

105. As a direct and proximate result of MGM's negligence *per se*, Plaintiffs and class members have suffered, and continue to suffer, damages arising from the Data Breach as set forth above.

106. Plaintiffs and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

107. Plaintiffs and class members are also entitled to the injunctive relief set forth above.

COUNT III

BREACH OF IMPLIED CONTRACT

(On Behalf of the Nationwide Class and all State Sub-Classes)

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

109. When Plaintiffs and class members provided their PII to MGM in exchange for MGM's services, they entered into implied contracts with MGM under which MGM agreed to take reasonable steps to protect their PII.

110. MGM solicited and invited Plaintiffs and class members to provide their PII as part of MGM's regular business practices. Plaintiffs and class members accepted MGM's offers and provided their PII to MGM.

111. When entering into the implied contracts, Plaintiffs and class members reasonably believed and expected that MGM's data security practices complied with relevant laws, regulations, and industry standards.

112. MGM's implied promise to safeguard PII is evidenced by, *e.g.*, the representations in MGM's Privacy Policy set forth above.

113. Plaintiffs and class members paid money for MGM's services. Plaintiffs and class members reasonably believed and expected that MGM would use part of those funds to obtain adequate data security. MGM failed to do so.

114. 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.

115. Plaintiffs and class members fully performed their obligations under the implied contracts by paying money to MGM.

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

117. As a result of MGM's conduct, Plaintiffs and class members have suffered, and continue to suffer, damages arising from the Data Breach as set forth above.

118. Plaintiffs and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

119. Plaintiffs and class members are also entitled to the injunctive relief set forth above.

COUNT IV

UNJUST ENRICHMENT

(On Behalf of the Nationwide Class and all State Sub-Classes)

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

121. This claim is plead in the alternative to the breach of implied contract claim.

122. Plaintiffs and class members conferred a monetary benefit on MGM. Specifically, they purchased services from MGM and in doing so provided MGM with their PII. In exchange, Plaintiffs and class members should have received from MGM the services that were the subject of the transaction as well as adequate protection of their PII.

123. MGM knew that Plaintiffs and class members conferred a monetary benefit, which MGM accepted. MGM profited from these transactions and used the PII for business purposes.

124. The amounts Plaintiffs and class members paid to MGM for its services were intended to be used, in part, to pay for MGM's administrative costs of data security.

125. Under the principles of equity and good conscience, MGM should not be permitted to retain the full monetary benefit of the transaction because MGM failed to implement appropriate data security measures.

126. MGM failed to adequately secure consumers' PII and, therefore, did not provide the full services that consumers paid for.

127. 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.

128. 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.

129. Plaintiffs and class members have no adequate remedy at law.

130. As a direct and proximate result of MGM's conduct, Plaintiffs and class members have suffered and will suffer injury and damages as set forth above.

131. 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 NRS 41.600

(On Behalf of the Nationwide Class and Nevada Sub-Class)

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

133. MGM engaged in unfair and unlawful acts and practices by failing to maintain adequate data security procedures, and permitting access to consumer information by data thieves, for whom MGM had no reasonable grounds to believe would be used for a proper purpose.

134. MGM violated the Nevada Consumer Fraud Act by engaging in unfair and unlawful acts and practices that constitute acts of "consumer fraud" as defined in NRS 41.600(2)(e) with respect to the goods and services it provided to the Nationwide Class and Nevada Sub-Class, including but not limited to the following:

a. by representing that it would maintain adequate data security practices to

safeguard consumer information from unauthorized disclosures, data breaches, and theft;

b. by omitting and concealing the material fact of the inadequacy of MGM's data security protections for consumers' PII;

c. by failing to disclose that MGM's data security systems failed to meet legal and industry standards for the protection of consumers' PII; and

d. by soliciting and collecting PII with knowledge that the information would not be adequately protected and by storing that PII in an unsecure electronic environment.

135. Plaintiffs and class members relied on MGM's implied promise of data security when providing their PII to MGM.

136. MGM's conduct violated NRS 598.0917(7) because it constituted a tender of "goods advertised for sale . . . or tendering terms of sale or lease less favorable than the terms advertised," *i.e.*, goods offered for sale without the corresponding promise that the consumer's PII would be kept reasonably secure.

137. MGM's violations of NRS 598.0917(7) constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

138. MGM also breached its duty under NRS 603A.210, which requires any data collector that "maintains records which contain personal information" of Nevada residents to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." MGM did not take such reasonable security measures, as shown by a system-wide breach of its data security systems.

139. Additionally, NRS 598.0923(3) provides that a violation of any federal or Nevada law constitutes consumer fraud. Thus, MGM's violations of the FTCA, NRS 598.0917(7), and NRS 603A violated NRS 598.0923(3).

140. MGM' violations of NRS 598.0923(3), NRS 598.0917(7), and NRS 603A in turn constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

141. MGM engaged in an unfair practice by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiffs and class members.

142. As a direct and proximate result of the foregoing, Plaintiffs and class members suffered injuries, including but not limited to actual damages and being denied a benefit conferred on them by the Nevada legislature.

143. As a result of these violations, Plaintiffs and class members are entitled to an award of actual damages, injunctive relief preventing MGM from continuing to violate data security requirements, and an award of reasonable attorneys' fees and costs.

COUNT VI

VIOLATION OF THE LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW La. Rev. Stat. Ann. §§ 51:1401, *et seq.*

(On Behalf of the Louisiana Sub-Class)

144. Plaintiff Wukovits re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

145. MGM, Plaintiff Wukovits, and the Louisiana Sub-Class members are "persons" within the meaning of the La. Rev. Stat. Ann. § 51:1402(8).

146. Plaintiff and the Louisiana Sub-Class members are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

147. MGM engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

148. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes the following conduct unlawful: "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

149. MGM participated in unfair and deceptive acts and practices that violated the Louisiana CPL, including by:

a. Failing to implement reasonable data security measures to protect consumers' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of PII, including duties imposed by the FTCA, 15 U.S.C. § 45;

c. Misrepresenting that it employed reasonable data security measures and would reasonably protect the privacy of consumers' PII;

d. Omitting and concealing the material fact that it did not employ reasonable measures to secure PII; and

e. Omitting and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security of PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

150. MGM's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of MGM's data security practices.

151. MGM intended to mislead Plaintiff and Louisiana Sub-Class members and/or induce them to rely on MGM's misrepresentations and omissions.

152. MGM's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Louisiana Sub-Class members that those individuals could not reasonably avoid. The substantial injury outweighed any benefits to consumers or to competition.

153. MGM acted intentionally, knowingly, and maliciously in violating the Louisiana CPL, and recklessly disregarded consumers' rights.

154. Had MGM disclosed that its data systems were not secure and were vulnerable to attack, MGM would have been unable to continue in its then-current state of business and would have been forced to adopt reasonable data security measures. Instead, MGM received, maintained, and compiled consumers' PII as part of the services MGM provided and for which

consumers paid, without advising consumers that MGM's data security practices were materially deficient.

155. Accordingly, Plaintiff and the Louisiana Sub-Class members acted reasonably in relying on MGM's misrepresentations and omissions, the truth of which they could not have discovered on their own.

156. As a direct and proximate result of MGM's unfair and deceptive acts and practices, Plaintiff and the Louisiana Sub-Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and non-monetary damages, as set forth above.

157. Plaintiff and the Louisiana Sub-Class members seek all monetary and non-monetary relief allowed by law, including actual damages, and treble damages for MGM's knowing violations of the Louisiana CPL, restitution, declaratory relief, attorneys' fees, and any other relief that is just and proper.

COUNT VII

VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW N.Y. Gen. Bus. Law §§ 349, *et seq.*

(On Behalf of the New York Sub-Class)

158. Plaintiff Kerri Shapiro re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

159. MGM engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including by:

a. Failing to implement reasonable data security measures to protect consumers' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of PII, including duties imposed by the FTCA, 15 U.S.C. § 45;

c. Misrepresenting that it employed reasonable data security measures and would reasonably protect the privacy of consumers' PII;

d. Omitting and concealing the material fact that it did not employ reasonable measures to secure PII; and

e. Omitting and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security of PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

160. Plaintiff and members of the New York Sub-Class were deceived in New York. They also transacted with MGM in New York by making hotel reservations from New York.

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

162. MGM acted intentionally, knowingly, and maliciously in violating New York's General Business Law, and recklessly disregarded consumers' rights.

163. As a direct and proximate result of MGM's deceptive and unlawful acts and practices, Plaintiff and New York Sub-Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as set forth above.

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

165. MGM's deceptive and unlawful practices caused substantial injury to Plaintiff and New York Sub-Class members that those individuals could not reasonably avoid.

166. Plaintiff and the New York Sub-Class members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages up to $1,000, restitution, injunctive relief, and attorney's fees and costs pursuant to N.Y. Gen. Bus. Law § 349(h).

COUNT VIII

VIOLATION OF THE OHIO DECEPTIVE TRADE PRACTICES ACT
Ohio Rev. Code §§ 4165.01, *et seq.*

(On Behalf of the Ohio Sub-Class)

167. Plaintiff Julie Mutsko re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

168. MGM, Plaintiff Mutsko, and the Ohio Sub-Class members are each a "person," as defined by Ohio Rev. Code § 4165.01(D).

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

170. MGM engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including by:

a. Representing that its goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7);

b. Representing that its goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9); and

c. Advertising its goods and services with intent not to sell them as advertise, in violation of Ohio Rev. Code § 4165.02(A)(11).

171. MGM's deceptive trade practices include:

a. Failing to implement reasonable data security measures to protect consumers' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of PII, including duties imposed by the FTCA, 15 U.S.C. § 45;

c. Misrepresenting that it employed reasonable data security measures and would reasonably protect the privacy of consumers' PII;

d. Omitting and concealing the material fact that it did not employ reasonable measures to secure PII; and

e. Omitting and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security of PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

172. 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.

173. MGM intended to mislead Plaintiff and Ohio Sub-Class members and/or induce them to rely on its misrepresentations and omissions.

174. MGM acted intentionally, knowingly, and maliciously in violating the Ohio Deceptive Trade Practices Act, and recklessly disregarded consumers' rights.

175. As a direct and proximate result of MGM's deceptive trade practices, Plaintiff and Ohio Sub-Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as set forth above.

176. Plaintiff and Ohio Sub-Class members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, attorneys' fees, and any other relief that is just and proper.

COUNT IX

VIOLATION OF THE SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT, S.C. Code Ann. §§ 39-5-10, *et seq.*

(On Behalf of the South Carolina Sub-Class)

177. Plaintiff Larry Lawter re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

178. MGM is a "person" as defined by S.C. Code Ann. § 39-5-10(a).

179. The South Carolina Unfair Trade Practices Act prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. § 39-5-20.

180. MGM advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting residents of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

181. MGM engaged in unfair and deceptive acts and practices, including by:

a. Failing to implement reasonable data security measures to protect consumers' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of PII, including duties imposed by the FTCA, 15 U.S.C. § 45;

c. Misrepresenting that it employed reasonable data security measures and would reasonably protect the privacy of consumers' PII;

d. Omitting and concealing the material fact that it did not employ reasonable measures to secure PII; and

e. Omitting and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security of PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

182. MGM's acts and practices had, and continue to have, the tendency or capacity to deceive.

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

184. MGM intended to mislead Plaintiff and South Carolina Sub-Class members and/or induce them to rely on its misrepresentations and omissions.

185. Had MGM disclosed to consumers that its data systems were not secure and, thus,

vulnerable to attack, MGM would have been unable to continue in its then-current state of business and would have been forced to adopt reasonable data security measures. Instead, MGM received, maintained, and compiled consumers' PII as part of the services MGM provided and for which consumers paid, without advising consumers that MGM's data security practices were materially deficient.

186. Plaintiff and the South Carolina Sub-Class members acted reasonably in relying on MGM's misrepresentations and omissions, the truth of which they could not have discovered on their own.

187. MGM had a duty to disclose the above-described facts due to the sensitivity and volume of PII in its possession. Such a duty is also implied by law due to the nature of the relationship between consumers and MGM, because consumers are unable to fully protect their interests with regard to their PII in MGM's possession. MGM's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the PII in its systems;

b. Active concealment of the state of its data security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, while purposefully withholding material facts from consumers that contradicted these representations.

188. MGM's business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. MGM's acts and practices offend established public policies that seek to protect consumers' PII and ensure that entities entrusted with PII use appropriate data security measures. These public policies are reflected in laws such as the FTCA, 15 U.S.C. § 45, and the South Carolina Data Breach Security Act, S.C. Code § 39-1-90, *et seq.*

189. MGM's unfair and deceptive acts or practices adversely affected the public interest because such acts or practices had the potential for repetition; MGM engaged in such acts or practices as a general rule; and such acts or practices impacted the public at large,

including the many South Carolina residents impacted by the Data Breach.

190. MGM's unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions and inactions occurred in the past, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, MGM's policies and procedures, such as its security practices, create the potential for recurrence of the complained-of business acts and practices.

191. MGM's violations present a continuing risk to Plaintiff and the South Carolina Sub-Class members as well as to the general public.

192. MGM intended to mislead Plaintiff and South Carolina Sub-Class members and/or induce them to rely on its misrepresentations and omissions.

193. MGM acted intentionally, knowingly, and maliciously in violating South Carolina's Unfair Trade Practices Act, and recklessly disregarded consumers' rights. Past data breaches in the hotel industry put MGM on notice of the potential for cyber-theft targeting its data networks. In light of these facts, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct, and would deter MGM and others from committing similar conduct in the future.

194. As a direct and proximate result of MGM's unfair and deceptive acts or practices, Plaintiff and the South Carolina Sub-Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as set forth above.

195. Plaintiff and South Carolina Sub-Class members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses, treble damages, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

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. Injunctive relief requiring MGM to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all class members;

E. An award of compensatory damages, statutory damages, and punitive damages;

F. An award of costs and expenses;

G. An award of attorneys' fees; and

H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

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

Dated: March 13, 2020

Respectfully submitted,

/s/ Don Springmeyer

WOLF, RIFKIN, SHAPIRO, SCHULMAN AND RABKIN, LLP
Don Springmeyer
3556 E Russell Rd
Second Floor
Las Vegas, NV 89120-2234
702-341-5200
Fax: (702) 341-5300
Email: dspringmeyer@wrslawyers.com

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

BERGER MONTAGUE PC
Michael Dell'Angelo
(*Pro Hac Vice to be submitted)*
Jon Lambiras (*Pro Hac Vice to be submitted)*
Joshua T. Ripley (*Pro Hac Vice to be submitted)*
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000

Fax: (215) 875-4604
mdellangelo@bm.net
jlambiras@bm.net
jripley@bm.net

MCCULLEY MCCLUER PLLC
Stuart McCluer (*Pro Hac Vice to be submitted)*
R. Bryant McCulley (*Pro Hac Vice to be submitted)*
Frank B. Ulmer (*Pro Hac Vice to be submitted)*
701 East Bay Street, Suite 411
Charleston, SC 29403
Tel: (843) 444-5404
Fax: (843) 444-5408
smccluer@mcculleymccluer.com
bmcculley@mcculleymccluer.com
fulmer@mcculleymccluer.com

Counsel for Plaintiffs and the Proposed Class