**TANASI LAW OFFICES**
Richard Tanasi, Esq.
8716 W. Spanish Ridge Ave. Suite 105
Las Vegas, NV 89148
Telephone: 702-906-2411
Facsimile: 866-299-4274
rtanasi@tanasilaw.com

**MORGAN & MORGAN COMPLEX LITGATION GROUP**
John A. Yanchunis (*pro hac vice to be submitted*)
Jean S. Martin (*pro hac vice to be submitted*)
Marcio Valladares (*pro hac vice to be submitted*)
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@forthepeople.com
jeanmartin@forthepeople.com
mvalladares@forthepeople.com

**LAW OFFICE OF PAUL C. WHALEN, P.C.**
Paul C. Whalen (*pro hac vice to be submitted*)
768 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870
paul@paulwhalen.com

*Additional Counsel Listed On Signature Page*

**UNITED STATES DISTRICT COURT**

**DISTRICT OF NEVADA**

| | |
|---|---|
| **JOHN SMALLMAN, ON BEHALF OF HIMSELF AND ALL OTHERS SIMILARLY SITUATED,**<br><br>**Plaintiff,**<br><br>**v.**<br><br>**MGM RESORTS INTERNATIONAL,**<br><br>**Defendant.** | **CASE NO.:**<br><br>**CLASS ACTION**<br><br>**COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY AND INJUNCTIVE RELIEF**<br><br>**JURY DEMAND** |

Plaintiff John Smallman ("Plaintiff"), individually, by and through the undersigned counsel, brings this class action lawsuit against MGM Resorts International ("Defendant," or "MGM"), on behalf of himself and all others similarly situated, and allege, based upon information and belief and the investigation of his counsel as follows:

## INTRODUCTION

1. MGM Resorts International is a global hospitality and entertainment company operating destination resorts throughout the world. Millions of people stay in MGM Resort properties every year, and in so doing provide MGM with a host of their personally identifiable information ("PII").[1]

2. In late 2019, MGM revealed that earlier in the summer an unauthorized individual accessed MGM's computer network system, downloaded customer data and then posted part of the data on a closed internet forum ("Data Breach").

3. The PII exposed in the Data Breach included, among other things: customer names, addresses, driver's license numbers, passport numbers, military identification numbers, phone numbers, emails and dates of birth.

4. MGM has indicated that, on or about September 5, 2019, it notified affected customers that their PII had been exfiltrated, but assured them that "there is no evidence that your information has been misused." Seeking to avoid additional negative publicity on the heels of the mass shooting that occurred 8 months earlier, MGM avoided bringing the matter to public light, hoping that the Breach and its inadequate cyber security practices would go unnoticed.

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

5. Unfortunately, the miscreants that took and/or acquired the sensitive PII had other plans, and on February 19, 2020, internet technology publication ZDNet revealed that the personally identifiable information of more than 10.6 million MGM hotel guests had been posted on a popular internet hacking forum, available for misuse by a host of bad actors.

6. MGM acknowledged that the exposed PII was a result of the Data Breach that occurred in the summer of 2019.

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

8. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard customer PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

9. As a result of Defendant's failure to implement and follow basic security procedures, MGM customer PII is now in the hands of thieves. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach, and will forever be at a heightened risk of identity theft and fraud.

10. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence, breach of implied contract, unjust enrichment, breach of confidence and violation of the Nevada Consumer Fraud Act and seeks to compel Defendant to adopt reasonably sufficient security practices to safeguard customer PII that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future.

## PARTIES

11. Plaintiff John Smallman is a resident of California and an MGM customer. Over the last 10 years, Plaintiff Smallman has stayed at the Luxor, giving copies his driver's license, as well as payment card and other PII. During his visits to Las Vegas, Plaintiff Smallman also used his payment cards at Bellagio.

12. Plaintiff suffered actual injury from having their PII stolen as a result of the Data Breach including, but not limited to: (a) paying monies to MGM for its goods and services which they would not have had if MGM disclosed that it lacked data security practices adequate to safeguard consumers' PII from theft; (b) damages to and diminution in the value of their PII—a form of intangible property that the Plaintiff entrusted to MGM as a condition of receiving MGM services; (c) loss of their privacy; (d) imminent and impending injury arising from the increased risk of fraud and identity theft.

13. As a result of the Data Breach, Plaintiff will continue to be at heightened risk for financial fraud and identity theft, and their attendant damages for years to come.

14. Defendant MGM Resorts International is a Delaware corporation headquartered at 3600 Las Vegas Blvd South Las Vegas, NV 89109. It is a global hospitality and entertainment company operating destination resorts throughout the world.

## JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are more than 10 million putative class members, many of whom have different citizenship from MGM.

16. This Court has jurisdiction over the Defendant which operates in this District, and the computer systems implicated in this Data Breach are likely based in this District.

17. Through its business operations in this District, MGM intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

18. 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 the District and has caused harm to Plaintiff and Class members residing in this District.

## STATEMENT OF FACTS

### *A. The MGM Data Breach*

19. On or about July 7, 2019, an unauthorized individual gained access to MGM Resorts International's computer network system, exfiltrated customer data, and then disclosed a subset of that data on a closed internet forum.

20. The data consisted of a treasure trove of MGM customer PII including: names, addresses, driver's license numbers, passport numbers, military identification numbers, phone numbers, emails and dates of birth.

21. Although the PII was subsequently removed from the closed internet site, in mid-February 2020 the seemingly full set of data containing the PII of more than 10.6 million MGM guests was published on a well-known hacking forum, visible to any number of dark web miscreants.

22. Internet security specialists recognized that the PII leaked in the Data Breach presents "a treasure trove" of contact details on customers, many of whom will now "face a higher risk of receiving spear-phishing emails, and being SIM swapped."[2] "The fact that the breach happened about seven months ago without any public disclosure may have led MGM to believe the data was

[2] ZDNet, Exclusive: Details of 10.6 million MGM hotel guests posted on a hacking forum, February 19, 2020, https://www.zdnet.com/article/exclusive-details-of-10-6-million-of-mgm-hotel-guests-posted-on-a-hacking-forum/

not going to be used by the thieves, but as with many breaches malicious actors sometimes wait months or years to tip their hand" presenting an ongoing problem for affected users.[3]

23. On or about September 5, 2019, MGM notified affected customers and various governmental agencies of the Data Breach, but otherwise kept news of the breach quiet. The Notice of Data Incident ("Notice") stated in relevant part.

**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. No customer financial information, passwords or credit cards were part of the data in question and it was taken down and removed from the closed internet site.

**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. Again, no financial information, passwords or credit cards were included in the database.

**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

[3] SC Magazine, February 20, 2020, MGM admits to 2019 data breach affecting 10.6 million customers, https://www.scmagazine.com/home/security-news/data-breach/mgm-admits-to-2019-data-breach-affecting-10-6-million-customers/

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.

***

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.[4]

### *B. MGM Privacy Policies*

24. MGM maintains a Privacy Policy wherein it details the PII it collects from customers and promises to maintain the security and integrity of such data.

MGM RESORTS PRIVACY POLICY[5]

MGM Resorts International values your patronage and respects your privacy. This Privacy Policy ("**Policy**") describes the information collection, use, protection, and sharing practices of MGM Resorts International and MGM Resorts International web sites, 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, e-mail address, and telephone number, and videos, recordings, and images of you ("**Personal Information**"). We may also obtain Personal Information from third parties.

**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

[4] Exhibit A.

[5] https://www.mgmresorts.com/en/privacy-policy.html

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 security measures are intended to protect these systems from unauthorized access. No security system is impenetrable and these systems could become accessible in the event of a security breach. 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.

25. Although MGM claims to employ "industry standard security measures," this representation, along with the promise to maintain the integrity of customer PII was belied by its failure to impose and maintain the necessary safeguards that would have prevented the Data Breach.

**C. Prevalence of Cyber Attacks and Susceptibility of the Hotel Industry**

26. In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year.[6] In 2017 a new record high of 1,579 breaches were reported representing a 44.7 percent increase over 2016.[7] The number of yearly data breaches have remained steady with 1,473 breaches reported in 2019.[8]

---

[6] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at* https://www.idtheftcenter.org/surveys-studys.

[7] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review, available at https://www.idtheftcenter.org/2017-data-breaches/.

[8] Identity Theft Resource Center, 2019 End -of-Year Data Breach Report. Available at https://www.idtheftcenter.org/2019-data-breaches/?utm_source=web&utm_medium=sitewidenotice&utm_campaign=01282020_2019DataBreachReport

27. The type of PII collected by companies by hotels makes this sector particularly to cyber-attack. Trustwave's "2018 Global Security Report" lists hospitality as one of the top three industries most vulnerable to payment card breaches while other estimates project that hotels are the unwelcome recipients of around 20 percent of all cyberattacks.[9] Indeed, in recent years, Marriott Hilton, Hyatt, and Trump hotels have all been cited for large-scale data negligence over the past few years. "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." *Id.*

28. "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."[10]

### *D. MGM Acquires, Collects, and Stores Plaintiff's and Class Members' PII*

29. As its Privacy Policy makes clear, MGM acquires, collects, and stores a massive amount of personally identifiable information on its customers.

30. As a condition of staying at its hotel properties, MGM requires that its customers entrust it with highly sensitive personal information.

---

[9] Hotel management, Why cybersecurity matters, https://www.hotelmanagement.net/tech/why-cybersecurity-matters

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

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

32. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

33. Plaintiff and the Class Members relied on MGM to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

### *E. The Value of Personally Identifiable Information and the Effects of Unauthorized Disclosure*

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

35. Personally identifiable information is a valuable commodity to identity thieves. As the FTC recognizes, with PII identity thieves can commit an array of crimes including identify theft, medical and financial fraud.[11] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites.

36. The ramifications of the MGM's failure to keep its customers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

37. "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

---

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

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…."[12]

38. At all relevant times, MGM knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences if its data security systems were breached, including, the significant costs that would be imposed on customers as a result of a breach.

### *F. MGM Fails to Comply with FTC Guidelines*

39. The Federal Trade Commission ("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.[13]

40. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[14] 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 someone is attempting to hack 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.

---

[12] SC Magazine, February 20, 2020, MGM admits to 2019 data breach affecting 10.6 million customers, https://www.scmagazine.com/home/security-news/data-breach/mgm-admits-to-2019-data-breach-affecting-10-6-million-customers/

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

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

41. 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.[15]

42. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data 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.

43. MGM failed to properly implement basic data security practices. MGM's failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

44. MGM was at all times fully aware of its obligation to protect the PII of customers because of its position as a trusted healthcare provider. MGM was also aware of the significant repercussions that would result from its failure to do so.

### *G. MGM Fails to Comply with Industry Standards*

45. Cyber security firms have routinely identified the hotel sector as one being particularly vulnerable to cyber-attacks because the of value of the PII which they maintain**.** These firms have promulgated a series of best practices that a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of

[15] FTC, *Start With Security*, *supra* note 19.

physical security systems; protection against any possible communication system; training hotel staff regarding critical points.[16]

46. MGM acknowledged the Data Breach was through a cloud server exposure. Although it did not state how or why the cloud server was exposed, "this could have easily been caused from poor cloud configuration and security hygiene…."[17]

***H. Plaintiff and Class Members Suffered Damages***

47. The ramifications of Defendant's failure to keep Customers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[18]

48. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

49. The Data Breach was a direct and proximate result of MGM's failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

---

[16] https://opendatasecurity.io/how-to-work-on-hotel-cyber-security/

[17] SC Magazine, February 20, 2020, MGM admits to 2019 data breach affecting 10.6 million customers, https://www.scmagazine.com/home/security-news/data-breach/mgm-admits-to-2019-data-breach-affecting-10-6-million-customers/

[18] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

50. Defendant is a multi-billion-dollar company and had the resources necessary to prevent the Breach, but neglected to adequately invest in data security measures, despite its obligation to protect customer data.

51. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into their systems and, ultimately, the theft of PII.

52. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[19]

53. To date, MGM has merely offered 12 months of identity monitoring services at no charge.[20] The offer, however, is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

54. Furthermore, Defendant's credit monitoring offer to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon

---

[19] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited April 19,2019).

[20] Exhibit A.

discovery of the breach, Defendant merely sent instructions "offering" the services to affected customers recommending they sign up for the services.

55. As a result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in their possession; and

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

56. In addition to a remedy for the economic harm, Plaintiff and the Class maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

### *I. Defendant's Delay in Identifying & Reporting the Data Breach Caused Additional Harm*

57. It is axiomatic that "[t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a

victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[21]

58. Indeed, once a data breach has occurred, "[o]ne 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. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves" (internal citations omitted).[22]

59. Although their PII was improperly exposed in July, affected customers were not notified of the Data Breach until September, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

60. As a result of MGM's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher.

## CLASS ACTION ALLEGATIONS

61. Plaintiff seeks relief on behalf of himself and as a representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons whose PII was compromised as a result of the Data Breach announced by MGM on or about September 5, 2019 (the "Class").

---

[21] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire, https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million.

[22] Consumer Reports, The Data Breach Next Door Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too, January 31, 2019, https://www.consumerreports.org/data-theft/the-data-breach-next-door/

62. Excluded from the Class are MGM and any of its affiliates, parents or subsidiaries; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned, their immediate families, and court staff.

63. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

64. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

65. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. The Data Breach implicates more than 10.6 million MGM customers.

66. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether MGM had a duty to protect customer PII;

b. Whether MGM knew or should have known of the susceptibility of its systems to a data breach;

c. Whether MGM's security measures to protect their systems were reasonable in light of best practices recommended by data security experts;

d. Whether MGM was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether MGM's failure to implement adequate data security measures allowed the breach of its data systems to occur;

f. Whether MGM's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unlawful exposure of the Plaintiff's and Class Members' PII;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of MGM's failure to reasonably protect its systems and data network; and

h. Whether Plaintiff and Class members are entitled to relief.

67. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff was an MGM customer whose PII was exposed in the Data Breach. Plaintiff's damages and injuries are akin to other Class Members, and Plaintiff seeks relief consistent with the relief sought by the Class.

68. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class he seeks to represent; is committed to pursuing this matter against MGM to obtain relief for the Class; and has no conflicts of interest with the Class. Moreover, Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation of this kind. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

69. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an individual Plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against MGM, and thus, individual litigation to redress MGM's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

70. MGM has physical and email addresses for Class members who therefore may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

71. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

72. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether MGM failed to timely notify the public of the Data Breach;
b. Whether MGM owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
c. Whether MGM's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
e. Whether Defendant failed to take commercially reasonable steps to safeguard customer PII; and
f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

73. 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.

**FIRST CAUSE OF ACTION**
**NEGLIGENCE**

74. Plaintiff restates and realleges paragraphs 1 through 73 above as if fully set forth herein.

75. As a condition of receiving services, Plaintiff and Class Members were obligated to provide MGM with their PII.

76. Plaintiff and the Class Members entrusted their PII to MGM with the understanding that MGM would safeguard their information.

77. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

78. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing the Defendant's security protocols to ensure that PII in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on cyber security measures regarding the security of such information.

79. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the current cyber scams being perpetrated and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiff and the Class.

80. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class Members.

81. Plaintiff and the Class Members had no ability to protect their PII that was in MGM's possession.

82. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

83. Defendant had a duty to put proper procedures in place in order to prevent the unauthorized dissemination Plaintiff and Class Members' PII.

84. Defendant has admitted that Plaintiff's and Class Members' PII was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

85. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding the Plaintiff's and Class Members' PII while it was within the MGM's possession or control.

86. Defendant improperly and inadequately safeguarded Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations and practices at the time of the Data Breach.

87. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its customers' PII.

88. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff and Class Members the existence, and scope of the Data Breach.

89. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

90. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class.

91. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and

correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

**SECOND CAUSE OF ACTION**
**NEGLIGENCE PER SE**

92. Plaintiff restates and realleges Paragraphs 1 through 73 as if fully set forth herein.

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

94. MGM violated Section 5 of the FTC Act 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 Plaintiff and Class Members.

95. MGM's violation of Section 5 of the FTC Act constitutes negligence per se as MGM's violation of the FTC Act establishes the duty and breach elements of negligence.

96. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

97. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act 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 and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

98. As a direct and proximate result of MGM's negligence per se, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial and medical

accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect.

99. Additionally, as a direct and proximate result of MGM's negligence per se, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in MGM's possession and is subject to further unauthorized disclosures so long as MGM fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

## THIRD CAUSE OF ACTION
## BREACH OF IMPLIED CONTRACT

100. Plaintiff restates and realleges paragraphs 1 through 73 above as if fully set forth herein.

101. Plaintiff and Class Members were required to provide their PII, including their names, addresses, dates of birth, telephone numbers, email addresses, and various forms of identification to Defendant as a condition of their use of Defendant's services.

102. Plaintiff and Class Members paid money to Defendant in exchange for services, along with Defendant's promise to protect their PII from unauthorized disclosure.

103. In their written privacy policies, MGM expressly promised Plaintiff and Class Members that they would only disclose PII under certain circumstances, none of which relate to the Data Breach.

104. MGM promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

105. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide protected health information and other PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) to prevent unauthorized disclosures of the PII, (d) to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) to reasonably safeguard and protect

the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) to retain the PII only under conditions that kept such information secure and confidential.

106. Without such implied contracts, Plaintiff and Class Members would not have provided their PII to Defendant.

107. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant, however, Defendant did not.

108. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' PII, which was compromised as a result of the Data Breach.

## FOURTH CAUSE OF ACTION
## UNJUST ENRICHMENT

109. Plaintiff restates and realleges paragraphs 1 through 73 above as if fully set forth herein.

110. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and in so doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

111. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

112. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

113. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to

implement appropriate data management and security measures that are mandated by industry standards.

114. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

115. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

116. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to Defendant's services.

117. Plaintiff and Class Members have no adequate remedy at law.

118. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

119. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

120. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In

the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

**FIFTH CAUSE OF ACTION**
**BREACH OF CONFIDENCE**

121. Plaintiff restates and realleges paragraphs 1 through 73 above as if fully set forth herein.

122. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of their use of Defendant's services.

123. Plaintiff and Class Members paid money to Defendant in exchange for services, along with Defendant's promise to protect their PII from unauthorized disclosure.

124. In its written privacy policies, MGM expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

125. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

126. Without such implied contracts, Plaintiff and Class Members would not have provided their PII to Defendant.

127. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendant, however, Defendant did not.

128. Defendant breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' PII, which was compromised as a result of the Data Breach.

**SIXTH CAUSE OF ACTION**
**VIOLATION OF NEVADA'S CONSUMER FRAUD ACT**
**Nevada Revised Statutes 41.600**

129. Plaintiff restates and realleges Paragraphs 1 through 73 as if fully set forth herein.

130. MGM engaged in unfair and unlawful acts and practices by failing to maintain adequate procedures to avoid a data breach, and permitting access to consumer reports by data thieves, for whom MGM had no reasonable grounds to believe would be used for a proper purpose. Plaintiff and Class members relied on MGM's implied promise of data security when providing their PII to MGM.

131. MGM 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 by credit card without the corresponding promise that a consumer's PII would be kept reasonably safe from harm.

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

133. 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 payment processing systems.

134. MGM also breached its duty under NRS 603A.215, which requires any data collector doing business in Nevada who accept payment cards in connection with a sale of goods or services to "comply with the current version of the . . . PCI Security Standards Council . . . with respect to those transactions." On information and belief, MGM failed to adhere to PCI standards, and was grossly negligent because the violation occurred in multiple stores across the United States.

135. MGM' violations of NRS 598.0923(3) constituted "consumer fraud" for purposes of NRS 41.600(2)(e).

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

137. 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).

138. MGM engaged in an unfair practice by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiff and Class Members.

139. As a direct and proximate result of the foregoing, Plaintiff and Class Members have suffered injuries including, but not limited to actual damages, and in being denied a benefit conferred on them by the Nevada legislature.

140. As a result of these violations, Plaintiff and Class Members are entitled to an award of actual damages, equitable injunctive relief preventing MGM to continue to violate the PCI DSS standards, as well as an award of reasonable attorney's fees and costs. Plaintiff and Class Members also seek declaratory relief pursuant to 28 U.S.C. § 2201, specifically an order declaring that MGM' data security procedures failed to meet the PCI DSS standards, which led to the exposure of the PII of Plaintiff and Class Members in the Data Breach.

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

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

b. An Order appointing Plaintiff as the class representative;

c. An Order appointing undersigned counsel as class counsel;

d. A mandatory injunction directing the Defendant to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;

e. An award of 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**

Plaintiff demands a jury trial as to all issues triable by a jury.

Dated: February 21, 2020

**s/_____**

**TANASI LAW OFFICES**
Richard Tanasi, Esq.
8716 W. Spanish Ridge Ave. Suite 105
Las Vegas, NV 89148
Telephone: 702-906-2411
Facsimile: 866-299-4274
rtanasi@tanasilaw.com

**MORGAN & MORGAN COMPLEX LITGATION GROUP**
John A. Yanchunis (*pro hac vice to be submitted*)
Jean S. Martin (*pro hac vice to be submitted*)
Marcio Valladares (*pro hac vice to be submitted*)
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@forthepeople.com
jeanmartin@forthepeople.com
mvalladares@forthepeople.com

**LAW OFFICE OF PAUL C. WHALEN, P.C.**
Paul C. Whalen (*pro hac vice to be submitted*)
768 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870
paul@paulwhalen.com

Brian P. Murray (*pro hac vice to be submitted*)
**GLANCY PRONGAY & MURRAY LLP**
230 Park Avenue, Suite 530
New York, NY 10169
Telephone: (212) 682-5340
Fax: (212) 884-0988
bmurray@glancylaw.com

*Attorneys for Plaintiff*