

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
 LITIGATION 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,**

Plaintiff,

v.

MGM RESORTS INTERNATIONAL,

Defendant.

CASE NO.:

CLASS ACTION

**COMPLAINT FOR DAMAGES,
 EQUITABLE, DECLARATORY AND
 INJUNCTIVE RELIEF**

JURY DEMAND

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

5 INTRODUCTION

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

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

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

16 4. MGM has indicated that, on or about September 5, 2019, it notified affected
17 customers that their PII had been exfiltrated, but assured them that “there is no evidence that your
18 information has been misused.” Seeking to avoid additional negative publicity on the heels of the
19 mass shooting that occurred 8 months earlier, MGM avoided bringing the matter to public light,
20 hoping that the Breach and its inadequate cyber security practices would go unnoticed.
21

22
23
24 ¹ Personally identifiable information generally incorporates information that can be used to
25 distinguish or trace an individual's identity, either alone or when combined with other personal or
26 identifying information 2 CFR § 200.79. At a minimum, it includes all information that on its face
27 expressly identifies an individual. PII also is generally defined to include certain identifiers that do
28 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).

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

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

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

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

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

21 10. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence,
22 breach of implied contract, unjust enrichment, breach of confidence and violation of the Nevada
23 Consumer Fraud Act and seeks to compel Defendant to adopt reasonably sufficient security practices
24 to safeguard customer PII that remains in its custody in order to prevent incidents like the Data
25 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.



Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.