CANADA

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

Nº : 500-06-001078-209

(Class Action)

SUPERIOR COURT

EVAN ZUCKERMAN

Plaintiff

v.

MGM RESORTS INTERNATIONAL

Defendant

ORIGINATING CLASS ACTION APPLICATION

IN SUPPORT OF HIS AUTHORIZED CLASS ACTION, THE REPRESENTATIVE PLAINTIFF RESPECTFULLY STATES THE FOLLOWING:

INTRODUCTION

1. By way of the Superior Court of Quebec's Authorization Judgment dated August 3, 2022 (the "**Authorization Judgment**"), the class action herein has been authorized against the Defendant and Plaintiff was appointed as the Representative Plaintiff representing all persons included in the Class described as follows:

> All persons in Quebec, including their estates, executors or personal representatives, whose personal and/or financial information was lost by and/or stolen from Defendant as a result of the data breach that occurred on or about July 7, 2019.

2. The main issues of fact and law to be treated collectively have been identified by this Honorable Court in the Authorization Judgment as follows:

   a) Was Defendant negligent and/or did Defendant commit a fault in the storing and safekeeping of the personal information of the Class Members whose information was ultimately compromised, lost and/or stolen on or before July 7, 2019?

   b) Did Defendant commit a fault and/or was negligent in the way in which it notified the Class Members about the Data Breach?

   c) Did Defendant commit a fault and/or was negligent in the delay in which it notified the Class Members about the Data Breach?

   d) Is Defendant liable to pay compensatory and/or moral damages to the Class Members as a result of the loss of said information, including without limitation actual monetary losses incurred, damages related to fraud or identity theft, decrease in credit score, out of pocket expenses, lost time, inconvenience, anxiety, fear, and stress, and if so in what amounts?

   e) Is Defendant liable to pay punitive and/or exemplary damages to the Class Members, and if so in what amount?

3. Defendant ("**MGM Resorts International**" or "**MGM**") is a Delaware (U.S.A.) corporation having its headquarters in the City of Las Vegas, Nevada, U.S.A., the whole as more fully appears from the Nevada Entity Information concerning MGM, communicated herewith as **Exhibit P-1**.

4. Defendant is well-known worldwide for building and operating luxurious resorts, casinos and hotels in the United States of America, most of which are located in Las Vegas, Nevada.

5. Plaintiff and millions of other consumers worldwide have stayed at one of Defendant's hotels in Las Vegas (and elsewhere) and therefore were forced to provide Defendant with their personal and financial information, including but not limited to their name, address, telephone number, email address, date of birth, credit card information, other identification, etc.

6. When a data breach affecting more than 142 million clients occurs, Defendant had the obligation to immediately and accurately notify its customers in order to help them prevent further fraud, identity theft, financial losses, losses of time, stress and inconvenience.

7. This authorized class action lawsuit stems from Defendant's failure to follow these obligations.

The Data Breach

8. On or about July 10, 2019, Defendant learned that its records and client information had been accessed and downloaded from an external cloud server by an unauthorized third party (the "**Data Breach**").

9. The Data Breach involves the Defendant's customers having stayed at the MGM's various locations, including but are not limited to the following:

- MGM Grand (Las Vegas);
- Aria (Las Vegas);
- Bellagio (Las Vegas);
- Circus Circus (Las Vegas);
- Excalibur (Las Vegas);
- Luxor (Las Vegas);
- Mandalay Bay (Las Vegas);
- The Mirage (Las Vegas);
- New York-New York (Las Vegas);
- Park MGM (Las Vegas);
- Signature at MGM Grand (Las Vegas);
- MGM Grand Detroit (Detroit, Michigan);
- Beau Rivage (Biloxi, Mississippi);
- Gold Strike Tunica (Tunica, Mississippi);
- Borgata (Atlantic City, New Jersey);
- MGM National Harbor (Prince George's County, Maryland);
- MGM Springfield (Springfield, Massachusetts).

10. Defendant chose not to inform all of the affected clients at that time in July 2019. Instead, in August 2019, Defendant downplayed the Data Breach by apparently only emailing a small number of affected clients, the whole as more fully appears from the multiple news articles reporting on the Data Breach, communicated herewith as **Exhibit P-2**, *en liasse*.

11. As reported in the P-2 news articles, Defendant only publicly acknowledged the Data Breach on or about February 2020, after the tech website Zdnet.com

published an article on February 19, 2020, confirming that "the MGM data dump that was shared today contains personal details for 10,683,188 former hotel guests."

12. And on July 14, 2020, various media outlets reported that the Data Breach affecting MGM's customers was even larger than previously reported and was now estimated to be affecting more than 142 million MGM customers worldwide, the whole as more fully appears from said articles, already communicated as **Exhibit P-3**, *en liasse*.

13. The P-3 articles of July 2020 also confirmed that at that time, the personal data of MGM's clients had already been offered for sale, and sold, on the "dark web".

14. Plaintiff was for the first time made aware of the Data Breach, almost a year later, when he received an email from MGM on June 12, 2020, the whole as more fully appears from the email sent by MGM to Plaintiff and presumably certain other Canadian Class Members, communicated herewith as **Exhibit P-4**.

15. Defendant therefore chose not to draw attention to the Data Breach and only started sending the P-4 emails in June 2020, namely after it was exposed and reported by the media that a very large amount of the MGM consumers information database was available on public forums.

16. In fact, after being exposed by the media in February 2020 (Exhibit P-2) Defendant still waited approximately four (4) additional months before sending the notification emails to certain Class Members, including the Plaintiff (Exhibit P-4).

17. Defendant did not send direct notification letters to the Class Members and there is presently no indication as to how many notification emails bounced back as undelivered, ended up in the Class Members' spam/junk folders and/or were otherwise not read by the Class Members.

18. Personal information is a valuable commodity. There is a "cyber black-market" available for criminals to openly post personal information on a number of Internet websites in what is known as the "dark web". This demand increases the likelihood of Class Members falling victim to identity theft.

19. Approximately two years later, namely in May 2022, it was reported online that the stollen data from the MGM Data Breach (namely 8.7 GB of files) had already been uploaded to the Telegram website and was readily available for free download by any and all ill-intended individuals.

20. Although Defendant had sent email notifications to some affected clients, there was (and still is) no information whatsoever related to the Data Breach in question on the MGM Resorts International website.

21. In addition, Defendant intentionally and in bad faith withheld and failed to divulge to the public, this Honorable Court, and the Class Members that the Class Members' unique "M Life" loyalty points program account number had also been stolen in the Data Breach. This important information was only discovered during the cross-examination of Defendant's affiant Elena Seiple, which was conducted in the present matter, at Plaintiff's request, on June 17, 2021.

22. The P-4 email to affected clients (including Plaintiff) confirms that Defendant purchased "a one-year subscription to the Equifax Complete Premier Plan" for clients who sign up.

23. This is a clear admission by Defendant that the Plaintiff and the Class Members were still (and had been for almost a year) at risk of fraud or identity theft.

24. In addition, every Class Member has or will justifiably experience stress, anxiety, inconvenience, loss of time, and/or fear due to the loss of personal information.

25. Defendant clearly failed to implement the proper steps and required IT security measures in order to safeguard and protect the Class Members' information.

26. By choosing not to immediately and automatically activate the credit monitoring services offered by Equifax Canada and TransUnion (the two credit agencies operating in Canada) and by not immediately and automatically posting the proper fraud alerts for all Class Members with said credit agencies, Defendant clearly chose to save money instead of helping protect the Class Members' files and identity.

27. Furthermore, the Defendant has not undertaken to indemnify the Class Members for damages suffered and has also not provided insurance coverage for losses incurred since the Data Breach and before its notification to the Class Members almost one year later.

28. Harm, inconvenience and damages suffered by victims of the Data Breach includes without limitation the following:

a) Fraud and/or identity theft, including fraudulent charges on their accounts and/or unreimbursed fees;

b) Professional fees disbursed;

c) Disbursements incurred such as for purchasing extra insurance or signing up for and paying for credit monitoring services;

d) Placing a fraud alert on their credit file, and costs related thereto;

e) Delays in the processing of any future requests or applications for credit in the future;

f) The obligation to closely monitor their accounts for possible fraud for all periods subsequent to the loss of information, which will be much longer than 12 months;

g) The obligation to be even more attentive than normally necessary concerning the communication of their personal information since they are at threat of social engineering and phishing, due to the higher possibility of fraudulent activity caused by Defendant's loss of the information;

h) The obligation to inform their financial institutions of the loss of the information by the Defendant and to deal with said financial institution in order to reduce risk of fraud as much as possible. In this regard, certain Class Members have and/or will close their accounts and open new accounts in order to protect themselves, which will cause further loss of time, inconvenience and costs;

i) Obtaining and reviewing their credit reports, regularly, in order to look for unauthorized transactions or fraud;

j) A negative effect on their credit score;

k) Loss of time and expenses related to (i) finding fraudulent charges; (ii) cancelling and reissuing cards or bank accounts; (iii) credit monitoring and identity theft prevention; (iv) imposition of withdrawal and purchase limits on compromised accounts; and (vi) the general nuisance and annoyance of dealing with all these issues resulting from the Data Breach.

29. In addition, Plaintiff and the Class Members have already and/or will continue to experience stress, anxiety, fear, inconvenience and/or loss of time due to the theft of their personal information.

30. Plaintiff and many Class Members have also paid or will pay certain fees or costs in order to further protect themselves, such as in order to activate a credit monitoring service or in order to purchase fraud insurance or alerts, title or other insurance, to change their personal information such as requesting new driver's licence numbers or Social Insurance Numbers, for credit protection consulting services, etc. Defendant is solely responsible for these costs or fees paid by the Class Members and for the inconvenience caused to Class Members in this regard.

31. Plaintiff and the Class Members are justified in claiming and have also been authorized to claim punitive damages against Defendant, as confirmed in the Authorization Judgment.

The Representative Plaintiff

32. Plaintiff has stayed at Defendant's hotel in Las Vegas, Nevada, U.S.A., and provided MGM with his personal and credit card information.

33. As mentioned above, Plaintiff received the email from Defendant on June 12, 2020 (Exhibit P-4) more than 11 months after the Data Breach had occurred and more than 11 months after Defendant was made aware of said Data Breach.

34. The Exhibit P-4 email from Defendant specifically confirms that Plaintiff's personal information was indeed part of the Data Breach in question and that his information was indeed stolen from Defendant's systems.

35. Plaintiff immediately signed up for the inadequate 1-year Equifax Canada credit monitoring services mentioned in the Exhibit P-4 email.

36. Before receiving this very late email notification, Plaintiff and many Class Members had not otherwise been made aware of the Data Breach.

37. Accordingly, in the case of Plaintiff and many other Class Members, these Class Members remained uninformed of the Data Breach during almost a year

after it occurred and remain highly vulnerable to fraud and identity theft. This represents additional faults and gross negligence by Defendant.

38. The Plaintiff and the Class Members, in good faith, were reasonably justified in assuming that Defendant would properly safeguard their personal information as part of the use of Defendant's renowned hotels and resorts, which Defendant clearly did not.

39. As a result of learning that his personal information was lost by Defendant, and subsequently offered for sale and sold on the dark web, Plaintiff experienced and continues to experience anxiety, stress, inconvenience, loss of time, and/or fear due to the loss of personal information.

40. Defendant negligently waited to provide its clients with the (limited and inadequate) Equifax Canada 12-month credit monitoring plan. This aggravated the risk that their private information would be used by malicious criminals.

41. In addition, considering that the personal information of over 142 million MGM clients have been stollen (including approximately 167,000 Class Members residing in Quebec), it will take much longer than 1 to 2 years for the thieve(s) to use and/or sell all of the stollen client information. Indeed, as mentioned above, the stollen data was later uploaded onto a public website approximately 2 years later and was offered for free download. Accordingly, credit monitoring services for only 1 year is wholly inadequate and will or has forced the Class Members to purchase additional coverage and insurance after the very short 12-month period has expired.

42. In fact, in order to help protect himself and his credit file from fraud and identity theft, Plaintiff did renew the Equifax Canada credit monitoring services on June 17, 2021 at a recurring monthly rate of $15.95 (plus taxes) per month, which Plaintiff has indeed personally paid for each month since June 2021, and which amounts Plaintiff hereby claims from Defendant as damages suffered as a direct result of the Data Breach herein, the whole as more fully appears from Plaintiff's proof of renewal of the Equifax protection dated June 17, 2021, communicated herewith as **Exhibit P-5**. Defendant is clearly responsible to indemnify and hold the Plaintiff and Class Members harmless of all losses and damages suffered well over twelve to twenty-four months since the Data Breach.

43. TransUnion and Equifax Canada are the two (2) only credit agencies in Canada, both of which Defendant failed to contact immediately about the Data Breach affecting Plaintiff and other Class Members.

44. In order to save money, Defendant has failed or refused to mandate and pay for TransUnion and Equifax Canada to immediately and automatically activate fraud alerts for all affected Class Members such as Plaintiff.

45. All fees payable to TransUnion or Equifax Canada in order to activate these alerts or other credit monitoring services are hereby claimed by Plaintiff and the Class Members from Defendant as damages.

46. Defendant is clearly responsible to indemnify and hold the Class Members harmless of all losses and damages suffered since the Data Breach.

47. Defendant had the obligation to ensure, by the most technologically sophisticated means possible and available, that said information was protected and could not be accessed. Defendant failed in this regard and failed to secure this private and highly sensitive information and their negligence and carelessness facilitated the Data Breach, making Defendant liable to pay compensatory, moral and punitive damages.

Punitive Damages

48. For all of the reasons more fully detailed above, including those contained in the Superior Court's August 3, 2022 Authorization Judgment herein, which are reiterated as though recited at length in the present section, Plaintiff respectfully submits that Defendant was grossly and/or intentionally negligent and is liable to pay punitive damages to the Class Members.

49. In fact, without limiting the generality of the forgoing, Defendant was grossly negligent and/or intentionally negligent when it :

    a. did not follow or properly implement an effective data security industry standard to protect the Class Members' personal information, which information MGM allowed to be accessed and downloaded from an external cloud server by unauthorized parties;

    b. failed to timely detect and prevent the Data Breach itself;

c. tried to downplay and hide the magnitude of the Data Breach for almost one year;

d. failed to promptly notify the Plaintiff and the Class Members of the Data Breach for almost one year, which in and of itself is abusive and egregious, justifying an award for such punitive damages;

e. failed to properly ensure that Plaintiff and Class Members are protected by credit monitoring services by both Equifax Canada and TransUnion and failing to post fraud alerts on the Class Members' credit files immediately after the Data Breach;

f. waited until after the media has exposed the fact that the personal information of millions of MGM clients was published on a hacking forum before notifying the Class Members, the whole as reported in the P-2 articles;

g. failed to provide assistance and relevant information about the Data Breach on its websites;

h. failed to even provide a telephone number for Class Members to call in order to access information about the Data Breach. Indeed, the 1 (888) 261-9692 telephone indicated in the P-4 emails only sends calls to Equifax Canada and not to MGM itself. Furthermore, the Equifax representatives who answer such calls are not able to confirm what information was actually stolen regarding the caller / Class Member in question;

i. failed to offer indemnification for losses suffered and proper coverage (including insurance) to Class Members;

j. failed to provide any updates to the Class Members after its investigation into the Data Breach;

k. intentionally and in bad faith withheld and failed to divulge to the public, this Honorable Court, and the Class Members that the Class Members' unique "M Life" loyalty points program account number had also been stolen in the Data Breach. This important information was only discovered during the cross-examination of Defendant's affidavit Elena

Seiple, which was conducted in the present matter, at Plaintiff's request, on June 17, 2021.

50. Defendant's excessive delays, faults and failures in the investigation and notification process after the Data Breach also further warrants and supports a condemnation for punitive damages herein.

51. Considering the above and considering the fact that Defendant has violated various laws which have been enacted in order to protect the Class Members' personal and/or financial information, Defendant is liable to pay punitive damages to all of the Class Members due to the loss of private information itself, aside from any other compensatory and moral damages suffered by the Class Members.

52. Defendant's above detailed actions qualify its fault as intentional which is a result of wild and foolhardy recklessness in disregard for the rights of the Class Members, with full knowledge of the immediate and natural or at least extremely probable consequences that its action would cause to the Class Members.

53. Defendant's negligence has shown a malicious, oppressive and high-handed conduct that represents a marked departure from ordinary standards of decency. In that event, punitive damages should be awarded to Class Members.

The Class Members

54. Class Members had their personal information lost by Defendant as described hereinabove, including without limitation names, email addresses, home address, date of birth, phone numbers.

55. Some Class Members incurred out of pocket expenses as a result of the Data Breach and/or as a result of receiving a notification, which expenses are claimed herein.

56. Class Members have experienced stress, anxiety, inconvenience, loss of time, and/or fear as a result of the Data Breach and/or as a result of receiving a notification letter.

57. Class Members had to closely monitor their accounts and credit files/reports, looking for possible fraud for all periods subsequent to the loss of information.

58. Class Members have been inconvenienced by the safety measures that became necessary in order to prevent further fraud exposure, such as signing up for credit monitoring service, posting an alert on their accounts or credit files, changing their personal information or account numbers, transferring money from one account to another, closing and opening accounts, paying for and dealing with NSF or other bank charges or interest, monitoring credit reports, etc.

59. Furthermore, Class Members who paid costs or fees in order to sign up for such credit monitoring, to post an alert on their accounts or credit files, to change their personal information, to purchase insurance, to hire consultants or professionals, or in order to otherwise protect themselves from further fraud exposure claim the reimbursement of these costs and fees from Defendant.

60. Class Members' credit score has and/or will be negatively affected as a result of the Data Breach, a further damage claimed herein.

61. Moreover, as mentioned above, it is likely that many Class Members have not been notified of the loss of their information, making them still at greater risk of fraud or identity theft.

62. Class Members can still fall victim to fraud or identity theft, in the future, due to Defendant's negligence in the safekeeping of their personal information.

63. The Representative Plaintiff and the Class Members are therefore justified and entitled to claim compensatory, moral and punitive damages against the Defendant.

64. The present action is well founded in fact and in law.

FOR THESE REASONS, MAY IT PLEASE THE COURT:

GRANT the Class Action of Plaintiff on behalf of all the Class Members against Defendant;

CONDEMN Defendant to pay to the Class Members compensatory damages for all monetary losses caused as a result of Defendant's loss of Class Members' information, and **ORDER** collective recovery of these sums;

CONDEMN Defendant to pay to the Class Members compensatory and/or moral damages, in the amount to be determined by the Court, as a result of Defendant's loss of Class Members' information, including without limitation for actual monetary losses incurred, damages related to fraud or identity theft, decrease in credit score, out of pocket expenses, lost time, inconvenience, anxiety, fear, and stress, and **ORDER** collective recovery of these sums;

CONDEMN Defendant to pay an amount in punitive / exemplary damages to every Class Member, in the amount to be determined by the Court, and **ORDER** collective recovery of these sums;

THE WHOLE with interest and additional indemnity provided for in the Civil Code of Quebec and with full costs and expenses including expert's fees and publication fees to advise Class Members.

MONTREAL, October 27, 2022

Lex Group Inc.

Lex Group Inc.
Per: David Assor and Sarah Rasemont
Class Counsel / Attorneys for the Representative Plaintiff
4101 Sherbrooke St. West
Westmount, (Québec), H3Z 1A7
Telephone: 514.451.5500 ext. 321
Fax: 514.940.1605

SUMMONS

(Articles 145 and following C.C.P.)

Filing of a judicial application

Take notice that the Plaintiff(s) has filed this application in the office of the Superior Court of Quebec in the judicial district of Montreal.

Defendant's answer

You must answer the application in writing, personally or through a lawyer, at the courthouse of Montreal, situated at 1, Notre-Dame Est, Montréal, Québec within 15 days of service of the application or, if you have no domicile, residence or establishment in Québec, within 30 days. The answer must be notified to the Plaintiff's lawyer or, if the Plaintiff is not represented, to the Plaintiff.

Failure to answer

If you fail to answer within the time limit of 15 or 30 days, as applicable, a default judgment may be rendered against you without further notice and you may, according to the circumstances, be required to pay the legal costs.

Content of answer

In your answer, you must state your intention to:

- negotiate a settlement;
- propose mediation to resolve the dispute;
- defend the application and, in the cases required by the Code, cooperate with the Plaintiff in preparing the case protocol that is to govern the conduct of the proceeding. The protocol must be filed with the court office in the district specified above within 45 days after service of the summons or, in family matters or if you have no domicile, residence or establishment in Québec, within 3 months after service;
- propose a settlement conference.

The answer to the summons must include your contact information and, if you are represented by a lawyer, the lawyer's name and contact information.

Change of judicial district

You may ask the court to refer the originating application to the district of your domicile or residence, or of your elected domicile or the district designated by an agreement with the Plaintiff.

If the application pertains to an employment contract, consumer contract or insurance contract, or to the exercise of a hypothecary right on an immovable serving as your main residence, and if you are the employee, consumer, insured person, beneficiary of the insurance contract or hypothecary debtor, you may ask for a referral to the district of your domicile or residence or the district where the immovable is situated or the loss occurred. The request must be filed with the special clerk of the district of territorial jurisdiction after it has been notified to the other parties and to the office of the court already seized of the originating application.

Transfer of application to Small Claims Division

If you qualify to act as a Plaintiff under the rules governing the recovery of small claims, you may also contact the clerk of the court to request that the application be processed according to those rules. If you make this request, the Plaintiff's legal costs will not exceed those prescribed for the recovery of small claims.

Calling to a case management conference

Within 20 days after the case protocol mentioned above is filed, the court may call you to a case management conference to ensure the orderly progress of the proceeding. Failing this, the protocol is presumed to be accepted.

Exhibits supporting the application

In support of the application, the Plaintiff intends to use the following exhibits:

Exhibit P-1: Nevada Entity Search Business Information online report regarding Defendant;

Exhibit P-2: Various news articles, *en liasse*;

Exhibit P-3: Various news articles, dated July 14, 2020 and July 15, 2020, *en liasse*;

Exhibit P-4: Notification email received by Plaintiff;

Exhibit P-5: Plaintiff's proof of renewal of the Equifax protection at $15.95 plus taxes per month, dated June 17, 2021.

These exhibits are available on request.

Notice of presentation of an application

If the application is an application in the course of a proceeding or an application under Book III, V, excepting an application in family matters mentioned in article 409, or VI of the Code, the establishment of a case protocol is not required; however, the application must be accompanied by a notice stating the date and time it is to be presented.

DO GOVERN YOURSELF ACCORDINGLY.

MONTREAL, October 27, 2022

Lex Group Inc.

Lex Group Inc.
Per: David Assor and Sarah Rasemont
Class Counsel / Attorneys for Representative Plaintiff