**C A N A D A**

(Class Action)

**PROVINCE OF QUEBEC**
**DISTRICT OF MONTREAL**

**SUPERIOR COURT**

**Nº : 500-06-001078-209**

**E[redacted] Z[redacted]**,

*Plaintiff*

v.

**MGM RESORTS INTERNATIONAL**,

*Defendant*

---

**AMENDED APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION**
**(Art. 574 C.C.P. and following)**

---

**TO ONE OF THE HONOURABLE JUDGES OF THE SUPERIOR COURT OF QUEBEC, SITTING IN AND FOR THE DISTRICT OF MONTREAL, THE PLAINTIFF STATES THE FOLLOWING:**

## INTRODUCTION

1. Plaintiff wishes to institute a class action on behalf of the following group, of which Plaintiff is a member, namely:

> All persons in Canada, 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, or any other Group(s) or Sub-Group(s) to be determined by the Court;
>
> (hereinafter, both Quebec resident and non-Quebec resident Class Members are collectively referred to as "**Class Member(s)**", "**Group Member(s)**", the "**Group**", the "**Class**", **"Consumers"** or "**Customers**").

2. 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 R-1**.

3. 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.

4. Plaintiff and millions of other consumers worldwide have stayed at one of Defendant's hotels in Las Vegas (and elsewhere) and therefore provided 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.

5. 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**").

6. 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).

7. 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 R-2**, *en liasse*.

8. According to the R-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 *inter alia* that:

> "[a]ccording to our analysis, the MGM data dump that was shared today contains personal details for 10,683,188 former hotel guests. Included in the leaked files are personal details such as full names, home addresses, phone numbers, emails, and dates of birth".

8.1. 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 R-5**, *en liasse*.

9. Plaintiff was for the first time made aware of the Data Breach, almost a year later, when he received a bilingual email from MGM on June 12, 2020, the whole as more fully appears from the email sent by MGM to Plaintiff and presumably other Canadian Class Members, communicated herewith as **Exhibit R-3**. The R-3 email states the following in its English version:

**From:** Customer Response <CustomerResponse@mgmresorts.com>
**Subject: Notice of Data Security Issue**
**Date:** June 12, 2020 at 11:12:08 AM EDT

---

Voir plus bas pour la version française de ce message.

MGM RESORTS INTERNATIONAL™

Dear Guest,

We are writing to notify you of an issue that involves your personal information. On July 10, 2019, we learned that an unauthorized party had accessed and downloaded certain MGM Resorts guest data from an external cloud server a few days earlier. The affected information may have included names, contact information (such as postal addresses, email addresses, and phone numbers),

and dates of birth. The specific data affected differed for each impacted individual.

Promptly after learning of the issue, we took steps to enhance our security measures such as by further strengthening our monitoring capabilities to detect unauthorized system activity. We engaged a leading third-party data security expert to assist with our investigation of the incident and coordinated with law enforcement authorities.

We recently identified that your information was affected by this issue. We take our obligation to safeguard personal information very seriously and are alerting you so you can take steps to help protect against the risk of misuse of your information. We are providing you with credit monitoring services for one year at no cost to you, and encourage you to follow the instructions below to enroll in these services.

We hope this information is useful to you. If you have any questions regarding this issue, please contact 1 (888) 261-9692 from 9:00 am - 5:00 pm, Eastern Time. We regret any inconvenience this may cause you.

Sincerely,

MGM Resorts International

---

**Credit Monitoring Enrollment Instructions**

We have purchased a one-year subscription to the Equifax Complete Premier Plan on your behalf.

- **Your unique Activation Code for the Equifax Complete Premier Plan is 859381208480.**

- Visit https://myservices.equifax.ca/prem to enroll using the Activation Code. No credit card is required for enrollment.
- Ensure that you enroll by **September 30, 2020** (the code will not work after this date).

With the Equifax Complete Premier Plan you can:

- Monitor your credit with regular reports and access to your Equifax credit score to notify you of unexpected changes.
- Work with a dedicated Customer Care Representative who will answer your questions.
- Help protect against theft of your personal information.
- Help minimize exposure. Your Equifax plan includes internet scanning and dark web monitoring.
- Help reduce financial risk with up to $50,000 of identity theft insurance.[1]

In addition, upon your request and at no cost, Equifax can place a fraud alert on your credit file. This is a notice that is placed on your credit report that alerts lenders and other companies who may extend you credit that your personal information may have been compromised. These companies may then take additional steps to verify your identity before issuing you credit.

[1] Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.



MGM Resorts International
3600 Las Vegas Boulevard South
Las Vegas, NV 89109

10. However, if a Class Members calls the 1 (888) 261-9692 telephone indicated in the R-3 emails, he or she is sent to Equifax Canada and not to MGM itself. Furthermore, after waiting a long time on the call for an actual Equifax representatives to answer the call, the agent is not able to confirm anything about what information was actually stolen regarding the caller / Class Member in question and the representative asks the caller to send an email to media@mgmresorts.com in order to ask specific questions about the Data Breach or the stolen information. This is clearly designed to force Class Members to jump through as many hoops as possible and to waste their time, the whole in order to have them give up and no longer continue with their inquiries and concerns against MGM.

11. In fact, Defendant chose not to draw attention to the Data Breach and only started sending the R-3 emails in June 2020, namely after it was reported by the media that a very large amount of the MGM consumers information database was available on public forums.

12. 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, making said Clients still a great risk of fraud and identity theft (having no knowledge of this risk).

13. 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.

14. The "dark web" is a part of the internet that is not indexed by search engines and has been described as a place where a "hotbed" of criminal activity occurs because of its difficulty to trace user activity.

15. Indeed, "dark web" users routinely buy and sell credit card numbers, all manners of drugs, guns, and other private information, including the private information now at issue in this class action.

16. As appears from R-2, the publication of the "data dump" on a "very popular and openly accessible hacking forum […] has brought it to many other hackers' attention" and created "a treasure trove for contact details of many high-profile" clients (including celebrities).

17. When a data breach affecting (…) more than 142 million Consumers 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.

18. This lawsuit stems from Defendant's failure to follow these obligations.

19. Indeed, and as mentioned above, although Defendant was made aware of the Data Breach as of at least July 2019, Defendant first tried to cover it up and downplay its magnitude by only sending a few emails in August 2019. However, after being exposed by the media in February 2020 (Exhibit R-2), Defendant still waited approximately four (4) additional months before sending the notification emails to certain Class Members, including the Plaintiff (Exhibit R-3).

20. Although Defendant has sent email notifications to some affected clients, there is presently no information whatsoever related to the Data Breach in question on the MGM Resorts International website.

20.1. 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 by the Plaintiff during his cross-examination of Defendant's affidavit Elena Seiple, which was conducted in the present matter, at Plaintiff's request, on June 17, 2021.

21. The R-3 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.

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

23. Plaintiff communicates herewith as though recited at length herein, as **Exhibit R-4**, *en liasse*, copies of various Class Action Complaints filed in the U.S.A. concerning the Data Breach, the whole in order to more fully fulfill the burden to demonstrate an arguable case herein.

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

25. 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.

26. 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.

27. Defendant's Customers have been and/or will be exposed to fraud and/or identity theft and these Customers have been harmed as a result. Harm to victims of the Data Breach includes without limitation fraudulent charges on their accounts, disbursements incurred such as for purchasing extra insurance, placing a fraud alert on their credit file, loss time and expenses related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards or bank accounts; (c) credit monitoring and identity theft prevention; (d) imposition of withdrawal and purchase limits on compromised accounts; and (e) the general nuisance and annoyance of dealing with all these issues resulting from the Data Breach.

28. On top of actual monetary losses related to fraud and identity theft, 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, which has made Plaintiff and the Class Members potential targets for fraud and/or identity theft.

29. The Class Members have suffered or will suffer certain additional inconveniences and damages including but not limited to the following:

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

    b) 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;

    c) 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;

    d) 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;

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

f) A negative effect on their credit score.

30. 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 invokes the following sections of provincial and federal legislation which apply under the circumstances and Plaintiff respectfully submits that the mere fact that the personal information was entrusted to the Defendant and subsequently lost by Defendant as detailed above constitutes an unlawful violation of the Class Members' fundamental rights, which makes Defendant liable to pay compensatory, moral and punitive damages:

a) Sections 3, 35, 36, 37 and 1621 of the *Civil Code of Quebec*, LRQ, c C-1991*;*

b) Sections 5 and 49 of the *Charter of Human Rights and Freedoms*, RDQ, c C-12;

c) Sections 1, 2, 10, 13 and 17 of the *Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, c P-39.1;

d) Sections 2, 3, 5 and 11 of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, as well as its sections 4.1, 4.3, 4.7 to 4.7.4 of its Schedule 1;

**FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY THE PLAINTIFF**

32. Plaintiff reiterates the above allegations in the present section, as though recited at length.

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

34. As mentioned above, Plaintiff received the email from Defendant on June 12, 2020 (Exhibit R-3) more than 11 months after the Data Breach had occurred and more than 11 months after Defendant was made aware of said Data Breach.

35. Plaintiff immediately signed up for the inadequate 1 year Equifax Canada credit monitoring services mentioned in the Exhibit R-3 email.

36. The Exhibit R-3 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.

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

38. 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.

39. 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.

40. As a result of learning that his personal information was lost by Defendant, Plaintiff experienced and continues to experience anxiety, stress, inconvenience, loss of time, and/or fear due to the loss of personal information.

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

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

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. Defendant's 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.

45. 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 that 1 to 2 years for the thieve(s) to use and/or sell all of the stollen

client information. Accordingly, credit monitoring services for only 1 year is wholly inadequate and will force the Class Members to purchase additional coverage and insurance after the very short 12 month period has expired, which Plaintiff indeed did on June 17, 2021 when he renewed the Equifax Canada credit monitoring services 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 **Exhibit R-6** which has already been communicated to Defendant on September 9, 2021. 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.

46. Plaintiff and the Class Members would not have used Defendant's services, providing their personal and financial information, if they had known that Defendant would be negligent and careless with the Customers' personal information.

**Punitive Damages:**

47. For all of the reasons more fully detailed above, 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.

48. 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. tried to downplay and hide the magnitude of the Data Breach for almost 1 year;

c. 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;

d. 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;

e. 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 R-2 articles;

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

g. 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 R-3 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;

h. failed to offer indemnification and proper coverage to Class Members.

i. 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 by the Plaintiff during his cross-examination of Defendant's affidavit Elena Seiple, which was conducted in the present matter, at Plaintiff's request, on June 17, 2021.

49. 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.

50. 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.

51. 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.

**FACTS GIVING RISE TO AN INDIVIDUAL ACTION BY EACH OF THE CLASS MEMBERS**

52. Plaintiff reiterates the above allegations in the present section, as though recited at length.

53. Every Class Member had his, her or its personal information lost by Defendant as described hereinabove, including without limitation names, email addresses, home address, date of birth, phone numbers (Exhibit R-2).

54. Every Class Member has or will experience stress, anxiety, inconvenience, loss of time, and/or fear due to the loss of personal information.

55. Every Class Member had and has to closely monitor his or her accounts ands credit files/reports, looking for possible fraud from now on and for all periods subsequent to the loss of information.

56. Every Class Member will be inconvenienced by any safety measures that may become 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.

57. Furthermore, every Class Member may be required to pay 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 for many subsequent years.

58. The Class Members' credit score has and/or will be negatively affected.

59. 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 great risk of fraud or identity theft. Indeed, sending mass email inevitably leads to bounced or undelivered emails and MGM has not otherwise notified the Class Members.

60. Every Class Member can still fall victim to fraud or identity theft, in the future, due to Defendant's negligence in the safekeeping of their personal information and negligence in the way it handled itself after being made aware of this Data Breach.

**CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION**

61. The composition of the Group makes it difficult or impracticable to apply the rules for mandates to sue on behalf of others or for consolidation of proceedings (Article 575 (3) C.C.P.) for the following reasons.

62. As mentioned above, it appears that Class Members' full names, email addresses, home address, date of birth, phone numbers, and other information had been lost, stolen or otherwise compromised as a result of the Data Breach.

63. Class Members are numerous and are scattered across the entire province and country since Defendant has received guests in its various locations from all around the country, including Quebec.

64. In addition, given the costs and risks inherent in an action before the Courts, many people will hesitate to institute an individual action against the Defendant. Even if the Class Members themselves could afford such individual litigation, the Court system could not as it would be overloaded. Further, individual litigation of the factual and legal issues raised by the conduct of the Defendant would increase delay and expense to all parties and to the Court system.

65. Moreover, a multitude of actions instituted risks leading to contradictory judgments on issues of fact and law that are similar or related to all Class Members.

66. These facts demonstrate that it would be impractical, if not impossible, to contact each and every Class Member to obtain mandates and to join them in one action.

67. In these circumstances, a class action is the only appropriate procedure for all of the Class Members to effectively pursue their respective rights and have access to justice.

68. The damages sustained by the Class Members flow, in each instance, from a common nucleus of operative facts, namely Defendant's negligence, and fault.

69. The claims of the Class Members raise identical, similar or related issues of law and fact (Article 575 (1) C.C.P.), namely:

    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?

70. The interests of justice favour that this application be granted in accordance with its conclusions.

## NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

71. The action that Plaintiff wishes to institute for the benefit of the Class Members is an action in damages.

72. The facts alleged herein appear to justify the conclusions sought by the Plaintiff (Article 575 (2) C.C.P.), namely the following conclusions that Plaintiff wishes to introduce by way of an originating application:

**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 determine 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.

73. Plaintiff suggests that this class action be exercised before the Superior Court in the District of Montreal for the following reasons:

a) Plaintiff resides in the District of Montreal;

b) A great number of Class Members such as Plaintiff reside in the judicial District of Montreal and/or provided their personal and financial information to Defendant in the District of Montreal;

c) A great number of Class Members such as Plaintiff used Defendant's websites and/or other websites to buy Defendant's services and complete the consumer transaction from and in the judicial District of Montreal;

d) Defendant through its website carries on business in the District of Montreal;

e) The R-3 notification email was received by Plaintiff and many other Class Members in the District of Montreal;

f) The undersigned attorneys representing the Plaintiff and the proposed Group practice in the District of Montreal.

74. Plaintiff, who is requesting to be appointed as Representative Plaintiff, is in a position to properly represent the Class Members (Article 575 (4) C.C.P.), since:

a) His personal information was provided to Defendant and was lost by Defendant as described hereinabove, Plaintiff having received the Exhibit R-3 notification emails confirming the theft of his personal information;

b) He has already and will continue to suffer anxiety, inconvenience, stress, loss of time, and fear, as well as out of pocket expense, as a result of said loss of information;

c) He may in the future fall, victim to fraud and/or identity theft because of Defendant's loss of her personal information;

d) He understands the nature of the action and has the capacity and interest to fairly and adequately protect and represent the interest of the Class Members;

e) He is available to dedicate the time necessary for the present action before the Courts of Quebec and to collaborate with Class Counsel in this regard and Plaintiff is ready and available to manage and direct the present action in the interest of the Class Members that Plaintiff wishes to represent;

f) Plaintiff has already been attributed the status of representative and authorized to represent data breach victims (by the Honourable Justice Stephen W. Hamilton (now of the Court of Appeal), in the context of another class action proceeding before this Honorable Court : Z[redacted] vs Target Corporation Inc., 500-06-000686-143, which file was ultimately settled;

g) Plaintiff is determined to lead the present file until a final resolution of the matter, the whole for the benefit of the Class Members;

h) His interests are not antagonistic to those of other Class Members;

i) He has given the mandate to the undersigned attorneys to obtain all relevant information to the present action and intends to keep informed of all developments;

j) He has given the mandate to the undersigned attorneys to post the present matter on their firm website in order to keep the Class Members informed of the progress of these proceedings and in order to more easily be contacted or consulted by said Class Members. In this regard, Plaintiff, though the undersigned attorneys, has already communicated, *en liasse*, as **Exhibit R-7**, **confidentially**, **under seal** and without waiving professional secrecy, the online submissions and comments received from multiple Class Members across the country, as though recited at length herein, for the purposes of further fulfilling the burden to demonstrate an arguable case at the authorization hearing herein;

k) He, with the assistance of the undersigned attorneys, is ready and available to dedicate the time necessary for this action and to collaborate with other Class Members and to keep them informed.

75. The present application is well founded in fact and in law.

**FOR THESE REASONS, MAY IT PLEASE THE COURT:**

**GRANT** the present Application;

**AUTHORIZE** the bringing of a class action in the form of an Application to institute proceedings in damages in the District of Montreal;

**APPOINT** the Plaintiff as the Representative Plaintiff representing all persons included in the Class herein described as:

> All persons in Canada, 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, or any other Group(s) or Sub-Group(s) to be determined by the Court;

**IDENTIFY** the principle issues of law and fact to be treated collectively as the following:

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

**IDENTIFY** the conclusions sought by the class action to be instituted as being the following:

**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 determine 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.

**DECLARE** that all Class Members who have not requested their exclusion from the Class in the prescribed delay to be bound by any Judgment to be rendered on the class action to be instituted;

**FIX** the delay of exclusion at 30 days from the date of the publication of the notice to the Class Members;

**ORDER** the publication or notification of a notice to the Class Members in accordance with Article 579 C.C.P., within sixty (60) days from the Judgment to be rendered herein in digital edition of the LaPresse, the Journal de Montreal, the Journal de Quebec, the Montreal Gazette, the Globe and Mail, and the National Post, and **ORDER** Defendant to pay for all said publication/notification costs;

**ORDER** that said notice be posted and available on the home page of Defendant's various websites, Facebook page(s), and Twitter account(s), and **ORDER** Defendants to send the notice by email with proof of receipt and by direct mail to all Class Members;

**THE WHOLE** with costs including without limitation the Court filing fees herein and all costs related to preparation and publication of the notices to Class Members.

**MONTREAL, (…) November 2, 2021**

**(S) Lex Group Inc.**

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

Nº.: 500-06-001078-209

**SUPERIOR COURT**
**(CLASS ACTION)**

**PROVINCE OF QUEBEC**
**DISTRICT OF MONTREAL**

**E[redacted] Z[redacted]**

*Plaintiff*

v.

**MGM RESORTS INTERNATIONAL**

*Defendant*

**AMENDED APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION**

**ORIGINAL**

*Me David Assor*


LEX GROUP
AVOCATS · ATTORNEYS
WWW.LEXGROUP.CA

**BL 5606**

**Lex Group Inc.**
4101 Sherbrooke St. West
Westmount, (Québec), H3Z 1A7

**T:** 514.451.5500 ext.321
**F:** 514.940.1605
@: davidassor@lexgroup.ca