C A N A D A

PROVINCE OF QUEBEC
DISTRICT OF MONTREAL

Nº : 500-06-001280-235

(Class Action)

SUPERIOR COURT

M. D.

Plaintiff

v.

MGM RESORTS INTERNATIONAL, legal person having its head office at 3600 Las Vegas Boulevard South, in the city of Las Vegas, Nevada, U.S.A., 89109

Defendant

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 September 11, 2023, 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. Millions of 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 September 11, 2023, Defendant published a post on its X (formerly Twitter) account: "MGM Resorts recently identified a cybersecurity issue affecting some of the company's systems". Plaintiff did not see that post and Defendant has since deleted the post although it is quoted in the TechCrunch article entitled "MGM Resorts blames 'cybersecurity issue' for ongoing outage", dated September 11, 2023, a copy of which is communicated herewith as **Exhibit R-2**.

6. The R-2 article confirmed that:

- "Hotel and casino giant MGM Resorts has confirmed a "cybersecurity issue" is to blame for an ongoing outage affecting systems at the company's Las Vegas properties.";

- "According to reports on social media, the incident has led to outages impacting ATM cash dispensers and slot machines at MGM's Las Vegas casinos, and forced hotel restaurants to accept cash-only payments. Guests also report that they cannot charge anything to their rooms and are unable to use their digital room keys.";

- "A notice on the MGM Resorts website — also affected by the ongoing outage — confirms that the incident impacts all of its Las Vegas resorts, including Aria, the Bellagio, Luxor, MGM Grand and Mandalay Bay. Guests are advised to call to make a reservation or to speak to a concierge."

- "A source with knowledge of the incident told TechCrunch that all of MGM's properties, including those outside of Las Vegas, appear to be affected by the

incident. The websites of several of MGM's regional resorts, including MGM Springfield in Massachusetts, MGM National Harbor and the Empire City Casino in New York, were all offline at the time of writing.".

7. On October 5, 2023, Defendant filed a "Current Report" with the United States Securities and Exchange Commission, a copy of which is communicated herewith as **Exhibit R-3**, admitting and confirming *inter alia* the following:

"**Item 7.01 Regulation FD Disclosure.**

On September 12, 2023, MGM Resorts International (the "Company") issued a statement that it had recently identified a cybersecurity issue affecting certain of the Company's U.S. systems.

Promptly after detecting the issue, the Company responded swiftly and shut down its systems to mitigate risk to customer information, which resulted in disruptions at some of the Company's properties but allowed the Company to prevent the criminal actors from accessing any customer bank account numbers or payment card information. Since that time, operations at the Company's domestic properties have returned to normal and virtually all of the Company's guest-facing systems have been restored. The Company continues to focus on restoring the remaining impacted guest-facing systems and the Company anticipates that these systems will be restored in the coming days.

The Company believes that the operational disruption experienced at its affected properties during the month of September will have a negative impact on its third quarter 2023 results, predominantly in its Las Vegas operations, and a minimal impact during the fourth quarter. The Company does not expect that it will have a material effect on its financial condition and results of operations for the year. Specifically, the Company estimates a negative impact from the cyber security issue in September of approximately $100 million to Adjusted Property EBITDAR for the Las Vegas Strip Resorts and Regional Operations, collectively. While the Company experienced impacts to occupancy due to the availability of bookings through the Company's website and mobile applications, it was mostly contained to the month of September which was 88% (compared to 93% in the prior year period). [...]. The Company has also incurred less than $10 million in one-time expenses in the third quarter related to the cybersecurity issue, which consisted of technology consulting services, legal fees and expenses of other third party advisors. Although the Company currently believes that its cybersecurity insurance will be sufficient to cover the financial impact to its business as a result of the operational disruptions, the one-time expenses described above and future expenses, the full scope of the costs and related impacts of this issue has not been determined.

Based on the ongoing investigation, the Company believes that the unauthorized third-party activity is contained at this time. The Company has determined, however, that the criminal actors obtained, for some of the Company's customers that transacted with the Company prior to March 2019, personal information (including name, contact information (such as phone number, email address and postal address), gender, date of birth and driver's license numbers). For a limited number of customers, Social Security numbers and passport numbers were also obtained by the criminal actors. The types of impacted information varied by individual. At this time, the Company

does not believe that customer passwords, bank account numbers or payment card information were obtained by the criminal actors. In addition, the Company does not believe that the criminal actors accessed The Cosmopolitan of Las Vegas systems or data. The Company also has no evidence that the data obtained by the criminal actors has been used for identity theft or account fraud. The Company has established a dedicated help line to address questions about this incident, which can be reached at 800-621-9437 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Please reference engagement number B105892 when calling. The Company also has set up a webpage www.mgmresorts.com/importantinformation with additional information. In the coming weeks, the Company will provide notification by email to individuals impacted by this issue as required by law and will offer those individuals free identity protection and credit monitoring services.

While no company can ever eliminate the risk of a cyber attack, the Company has taken significant measures, working with industry-leading third-party experts, to further enhance its system safeguards. These efforts are ongoing."

8. The URL mentioned by Defendant in its above-cited R-3 filing (www.mgmresorts.com/importantinformation) leads to a "Notice of Data Breach" dated October 5, 2023, a copy of which is communicated herewith as **Exhibit R-4**, which notice states the following:

"Notice of Data Breach

October 5, 2023

We recently learned of a cybersecurity issue affecting our company.

What Happened?

MGM Resorts International recently disclosed that the company identified a cybersecurity issue affecting certain of our systems and that our investigation into the issue was ongoing. On or around September 29, 2023, we determined that an unauthorized third party obtained personal information of some of our customers on September 11, 2023.

What Information Was Involved?

The affected information included name, contact information (such as phone number, email address, and postal address), gender, date of birth, and driver's license number. For a limited number of customers, Social Security number and/or passport number was also affected. The types of impacted information varied by individual.

We do not believe customer passwords, bank account numbers, or payment card information was affected by this issue.

What We Are Doing

Promptly after learning of this issue, we took steps to protect our systems and data, including shutting down certain systems. We also quickly launched an investigation with the assistance of leading

cybersecurity experts and are coordinating with law enforcement. We take the security of our systems and data very seriously and have put in place additional safeguards to further protect our systems.

MGM Resorts is notifying relevant customers by email as required by law and has arranged to provide those customers with credit monitoring and identity protection services at no cost to them. Individuals who receive an email from MGM Resorts about this issue should refer to that email for additional information and instructions for enrolling in these services.

What You Can Do

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your free credit reports. We also recommend that you remain alert for unsolicited communications involving your personal information.

If you are in the U.S. and would like to check your credit report, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. U.S. residents can order a free credit report by visiting www.annualcreditreport.com or calling toll-free at 1-877-322-8228. The U.S. Reference Guide below provides recommendations by the U.S. Federal Trade Commission on the protection of personal information.

We regret any inconvenience this issue may have caused. If you have any questions regarding this matter, please refer to the Frequently Asked Questions below or contact 1-800-621-9437 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Please reference engagement number B105892 when calling.

(...)

Frequently Asked Questions

To help answer questions you may have related to this matter, please refer to the FAQs below.

1. What happened?

MGM Resorts International recently disclosed that the company identified a cybersecurity issue affecting certain of our systems and that our investigation into the issue was ongoing. On or around September 29, 2023, we determined that an unauthorized third party obtained personal information of some of our customers on September 11, 2023.

2. What did MGM Resorts do when it discovered the issue?

Promptly after learning of this issue, we took steps to protect our systems and data, including shutting down certain systems. We also quickly launched an investigation with the assistance of leading cybersecurity experts and are coordinating with law enforcement. We take the security of our systems and data very seriously and have put in place additional safeguards to further protect our systems.

MGM Resorts is notifying relevant customers by email as required by applicable law and has arranged to provide those customers with credit monitoring and identity protection services at no cost to them. Individuals who receive an email from MGM Resorts about this issue should refer to that email for additional information and instructions for enrolling in these services.

3. What information has been compromised?

The affected information included name, contact information (such as phone number, email address, and postal address), gender, date of birth, and driver's license number. For a limited number of customers, Social Security number and/or passport number was also affected. The types of impacted information varied by individual.

We do not believe customer passwords, bank account numbers, or payment card information was affected by this issue.

For individuals who became MGM Resorts customers after February 2019, we do not believe sensitive personal information (such as driver's license number, passport number or Social Security number) was affected by this issue.

This issue did not affect personal information that customers provided in connection with their visit to The Cosmopolitan of Las Vegas.

4. What should I do to help protect my information?

We recommend that you:

- Remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your free credit reports.
- Remain alert for unsolicited communications involving your personal information.
- Order a credit report. If you are in the U.S. and would like to check your credit report, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. U.S. residents can order a free credit report by visiting www.annualcreditreport.com or calling toll-free at 1-877-322-8228.

5. Where can I get more information?

If you have additional questions regarding this matter, please contact us at 800-621-9437 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Please reference engagement number B105892 when calling.

6. What if I am in Canada?

On or about October 26, 2023, MGM determined that some Canadian customers were impacted. MGM issued notice to affected Canadian customers in accordance with applicable law. If you have received an email or letter from MGM, this includes the notice information that relates to you. Affected Canadian customers should review the information in the notice that they receive. For outstanding questions you may contact 1-855-984-2828. The call centre is available Monday to Friday, from 8:00 am ET to 8:00 pm ET. "

(Emphasis added)

9. Plaintiff had no reason to be consulting the Defendant's website in October 2023 or otherwise, and therefore he did not see Defendant's "Notice of Data Breach" (R-4).

10. In addition, although the R-4 Notice of Data Breach confirms that "MGM issued notice to

affected Canadian customers", no such notice had been sent at that time to Plaintiff and presumably the other Class Members.

11. Indeed, and notwithstanding Defendants promises to promptly notify the affected Canadian Class Members (in R-3 and R-4), Defendant abusively and excessively waited until November 27, 2023 to send an email notice to Plaintiff and some but not all affected Canadian Class Members.

12. Therefore, according to Defendant's Notice of Data Breach, Defendant learned that Canadians had been affected by the Data Breach as early as October 26, 2023 but Defendant chose to wait over an extra month before starting to send actual notices to Canadians affected clients, and well over 2 months since the Data Breach itself of September 11, 2023. These delays were excessive and constitute a further fault and negligence by the Defendant.

13. Indeed, on November 27, 2023, Defendant sent the following email to Plaintiff, a copy of which is communicated herewith as **Exhibit R-5**:

"**De:** MGM Resorts Cybersecurity Notification <mgmresortsnotification@cyberscout.com>
Date: 28 novembre 2023 à 08:02:43 HNE
À: […]@[…]
Objet: Avis concernant un incident de confidentialité

Veuillez lire ce message au complet.
Ne répondez pas au présent courriel, car il a été envoyé à partir d'une boîte de courriel automatique.

MGM RESORTS

27 Novembre 2023

AVIS CONCERNANT UN INCIDENT DE CONFIDENTIALITÉ IMPLIQUANT DES RENSEIGNEMENTS PERSONNELS

Cher/Chère […],

Nous avons récemment appris qu'un problème de cybersécurité affecte notre société.

Que s'est-il passé ?

MGM Resorts International (« MGM ») a récemment annoncé que la société avait identifié un problème de cybersécurité affectant certains de ses systèmes et qu'une enquête sur ce sujet

était en cours. Le ou vers le 26 octobre 2023, nous avons déterminé qu'un tiers non autorisé avait obtenu des renseignements personnels concernant certains de nos clients canadiens le ou vers le 11 septembre 2023.

Quels renseignements sont concernés ?

Les types de renseignements personnels concernés par ce problème de cybersécurité varient en fonction des personnes. D'après nos vérifications, les renseignements personnels vous concernant qui ont pu être affectés par ce problème font partie d'une ou plusieurs des catégories suivantes : votre nom, vos coordonnées (telles que votre numéro de téléphone, votre adresse de courriel et votre adresse postale), votre genre, votre date de naissance, et/ou la date d'anniversaire de votre mariage.

Nous ne croyons pas que les mots de passe, les numéros de compte bancaire ou les informations de carte de paiement aient été affectées par ce problème.

Ce que nous faisons

Dès que nous avons pris connaissance de ce problème, nous avons pris des mesures pour protéger nos systèmes et nos données, notamment en fermant certains systèmes. De plus, nous avons rapidement entamé une enquête en collaboration avec des experts en cybersécurité de premier plan et nous coordonnons nos efforts avec les autorités compétentes. Nous prenons la sécurité de nos systèmes et de nos données au sérieux et avons mis en place des mesures de protection supplémentaires pour mieux protéger nos systèmes.
Le guide référencé ci-dessous fournit des informations sur l'inscription et des recommandations pour la protection des renseignements personnels.

Ce que vous pouvez faire

Nous vous recommandons de rester vigilant face aux incidents de fraude et de vol d'identité en examinant vos relevés de compte pour toute activité inhabituelle et en surveillant vos fichiers de crédit personnels. Nous vous recommandons également de rester vigilant face à toute communication non sollicitée impliquant vos renseignements personnels.

Pour vous aider, MGM propose des services de surveillance du crédit.

myTrueIdentity®

Nous avons fait appel à TransUnion du Canada, Inc. (« TransUnion Canada »), une Société de TransUnion® et l'une des principales agences de renseignements sur les consommateurs au Canada.

Par l'entremise de TransUnion Canada, nous avons mis en place pour vous un abonnement de 12 mois à myTrueIdentity® de TransUnion, un service de surveillance en ligne, sans frais pour vous. Ce service de surveillance du crédit vous informera par courriel des changements importants apportés à votre dossier de crédit TransUnion Canada. Si vous recevez une alerte par courriel, vous pouvez examiner et valider le changement signalé en vous connectant au portail myTrueIdentity®. Cela vous permettra de déceler toute activité potentiellement frauduleuse sur votre rapport de crédit TransUnion Canada.

Nous vous encourageons à profiter de ce service en vous inscrivant en ligne. Pour activer votre service, rendez-vous sur cette page :

https://www.mytrueidentity.ca/fr

Vous serez invité à entrer le code d'activation suivant : […]

Veuillez vous assurer d'entrer votre code d'activation avant le 31/03/2024 afin de pouvoir profiter des avantages offerts par ce service.

Une fois le processus d'activation en ligne complété, vous aurez accès aux fonctionnalités suivantes :

- Un accès en ligne illimité au rapport de crédit TransUnion Canada, mis à jour quotidiennement. Un rapport de crédit est une image instantanée de vos antécédents financiers et l'un des principaux outils utilisés pour détecter le vol d'identité ou la fraude liée au crédit.
- Un accès en ligne illimité au pointage de risque CreditVision®, incluant une mise à jour quotidienne des facteurs et de l'analyse. Un pointage de crédit est un nombre à trois chiffres calculé selon les renseignements que contient votre dossier de crédit TransUnion Canada à un moment précis.
- Des alertes de surveillance du crédit par courriel signalant tout changement important sur votre rapport de crédit TransUnion Canada. Dans le monde virtuel d'aujourd'hui, les alertes de crédit sont un outil puissant pour vous aider à vous protéger contre l'usurpation d'identité, prendre rapidement des mesures contre toute activité potentiellement frauduleuse, et vous rassurer davantage.
- Un accès illimité à des ressources éducatives en ligne sur la gestion du crédit, l'aide aux victimes de fraude et la prévention du vol d'identité.
- Le service Surveillance du Dark Web offre une surveillance des sites Web de surface, sociaux, profonds, et cachés, à la recherche de renseignements personnels liés à l'identité et de nature financière possiblement exposés, afin de vous aider à vous protéger contre le vol d'identité.

Si vous avez besoin d'une assistance technique pour myTrueIdentity®, veuillez communiquer avec TransUnion Canada au 1 888 752 9131.

Rétablissement en cas de vol d'identité

Nous avons également pris des arrangements avec CyberScout (« CyberScout »), une Société TransUnion®, pour qu'elle fournisse des services de rétablissement en cas d'usurpation d'identité. Pendant votre abonnement de 12 mois au service de surveillance du crédit, les agents du centre d'appels de CyberScout seront disponibles pour répondre à vos questions sur le vol d'identité et la fraude. Dans le cas peu probable où vous seriez victime de fraude, un spécialiste de la fraude personnelle vous aidera à résoudre tout problème de vol d'identité, notamment en collaborant avec les agences, entreprises et institutions concernées. Ce service comprend :

- Un accès à un spécialiste de la fraude personnelle jusqu'à la résolution de la question.
- Une notification à toutes les agences gouvernementales et privées concernées.

- Une aide au dépôt d'un rapport auprès des forces de l'ordre, le cas échéant.
- Une création de dossiers complets pour les assurances et les forces de l'ordre.
- Une aide à l'examen des rapports de crédit pour détecter de possibles activités frauduleuses.
- Une assistance proactive pour répondre à vos questions sur la fraude, ou dans le cas où vous seriez victime de vol d'identité ou de fraude, ainsi qu'une assurance de remboursement des frais d'un montant de 1 000 000 $ 1.

Pour joindre un spécialiste de la fraude personnelle chez CyberScout, veuillez appeler le 1 855 984 2828. Le centre d'appels CyberScout peut être joint du lundi au vendredi, de 8 h à 20 h, l'heure de l'Est. Veuillez noter que le centre d'appels CyberScout ne sera pas en mesure de fournir de l'assistance pour toute question liée à myTrueIdentity®. Veuillez appeler la ligne d'assistance myTrueIdentity® pour obtenir une assistance technique.

Nous avons également mis en place des services de centre d'appels jusqu'au 18 février 2024. Pour joindre le centre d'appels, veuillez appeler le 1 855 984 2828. Le centre d'appels peut être joint du lundi au vendredi, de 8 h à 20 h, l'heure de l'Est.

Cordialement,

MGM Resorts International

1. Souscrite par certains souscripteurs de Lloyd's dans le cadre d'une police collective principale émise au nom de Cyberscout Limited, Sontiq Inc. et de toutes ses filiales au profit des membres du programme. L'assurance remboursement des frais n'est disponible qu'une fois l'inscription au service de surveillance du crédit en ligne effectuée. Veuillez consulter la page www.sontiq.com/terms-of-use pour plus de détails."

14. The Data Breach involves the Defendant's Customers having provided it with their personal and/or financial information including those who 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).

15. As mentioned in the email sent to the Plaintiff, Defendant indicated that it had set up a call center for affected clients to call. However, if a Class Members calls the 1 (855) 984-2828 telephone number indicated in the R-5 emails, he or she is sent to TransUnion Canada representatives and not to MGM itself. Furthermore, after waiting a long time on the call for an actual TransUnion representative 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, provides generic information about data breaches in general, and in fact tries to downplay the situation.

16. 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).

17. 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.

18. 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.

19. 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.

20. When a data breach affecting likely millions of consumers occurs, Defendant had the obligation to immediately and accurately notify its clients in order to help them prevent further fraud, identity theft, financial losses, losses of time, stress and inconvenience.

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

22. Indeed, and as mentioned above, although Defendant was made aware of the Data Breach as of at least September 11, 2023, Defendant still waited until the end of November 2023 before sending the notification emails to certain Class Members, including the Plaintiff (Exhibit R-5).

23. The R-5 email to affected clients (including Plaintiff) confirms that Defendant set up a one-year subscription to the TransUnion Canada mytrueidentity® service, for clients who sign up.

24. This is a clear admission by Defendant that the Plaintiff and the Class Members are at risk of fraud or identity theft.

25. In addition, in the R-5 emails, Defendant states that: "*Nous ne croyons pas que les mots de passe, les numéros de compte bancaire ou les informations de carte de paiement aient été affectées par ce problème*". Evidently, after over two months since the September 11, 2023 Data Breach, it is clear that Defendant simply does not know what was stolen, and most importantly and worrisome for the Class Members, Defendant cannot absolutely confirm that passwords, bank account numbers, credit card number and other payment card numbers have not been stolen, which increases the stress, fear and anxiety for the Class Members but also significantly raises the threat level for this Data Breach since the Class Members have no assurances as to what has indeed been stolen.

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

27. In this regard, this is not the first Data Breach incident for Defendant in recent years. Indeed, and in order to more fully fulfill the burden to demonstrate an arguable case herein including in relation to the claim for punitive damages, Plaintiff refers (as though recited at length) to the August 3, 2022 authorization Judgment rendered by this Honorable Court in Zuckerman vs. MGM Resorts International, 2022 QCCS 2914, a copy of which is communicated herewith as **Exhibit R-6**. That first data breach class action is in relation to a significant MGM Resorts International data breach which occurred in July of 2019 and which affected over 100 million customers worldwide (which includes approximately 2 million Canadian, of which over 160,000 are from Quebec).

28. Clearly, Defendant has not improved its IT security measures, programs and protocols after the July 2019 data breach since it permitted a much more significant data breach to occur in September 2023, which involved once again the theft of the Class Members personal and/or financial information. This constitutes additional intentional faults and

negligence by the Defendant which further justifies the claim for punitive damages herein.

29. In addition, many class members included in the authorized July 2019 MGM data breach class action file are also included in this most recent September 2023 Data Breach, which means that Defendant would have permitted their personal and financial information to be stolen at least twice, by at least 2 different unauthorized third parties, and this increases their damages and further warrants their claim for punitive damages.

30. Moreover, those individuals included in both MGM data breaches, who would have received the class action authorization notices in the Zuckerman file during the summer of 2023, followed by the R-5 MGM data breach notices in November 2023, are justifiably skeptical and will surely not sign up for the mytruidentity® protection since they will reasonably expect this to be fraudulent activity (including social engineering and phishing) stemming from the July 2019 data breach. This will cause them more loss of time, aggravation, fear and anxiety. In this regard, the Plaintiff communicates herewith, as **Exhibit R-7 (*en liasse,* under seal and confidentially - without waiving professional secrecy)**, the online submissions and comments already received from multiple Class Members before this case was instituted (as though recited at length herein), for the purposes of further fulfilling the burden to demonstrate an arguable case at the authorization hearing herein (Plaintiff reserving the right to file and rely upon further online submissions which may be received in the future from Class Members herein).

31. By choosing not to immediately and automatically activate the credit monitoring services offered by Equifax Canada and TransUnion Canada (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.

32. Furthermore, the Defendant has not undertaken to indemnify the Class Members for damages suffered and has also not provided adequate insurance coverage for losses incurred since the Data Breach.

33. 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.

34. 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.

35. 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.

36. 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 and/or renew 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.

37. When trying to sign up for the one-year mytrueidentity® program online, some Class Members experienced error messages and authentication problems rendering the activation code useless and forcing them to have to call TransUnion for assistance, representing additional loss of time and aggravation. In addition, when calling TransUnion, some Class Members were then asked to proceed to the ocs.transunion.ca website in order to "dispute inaccuracies" in the TransUnion Canada records about the credit file, which dispute process involves having to fill out forms, submit documents and IDs, and having to wait over 30 days for a response, all the while their credit files are not being secured or protected at all. This represents further loss time and aggravation caused by the MGM Data Breach and in addition, by forcing Class Members to have to jump through many hoops and/or submit additional information or documents in order to activate the credit monitoring service, this reduces the likelihood that Class Members will not actually complete the process (especially considering the first July 2019 MGM data breach).

38. All of this could have and should have been avoid by Defendant, by automatically activating fraud alerts and the credit monitoring services for the Class Members.

39. 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, 3.1 and following, 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

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

41. As mentioned above, Plaintiff received the email from Defendant (Exhibit R-5), more than 2 months after the Data Breach had occurred.

42. Plaintiff has provided MGM with his personal and credit card information. Indeed, the Exhibit R-5 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:

> "Quels renseignements sont concernés ?
>
> Les types de renseignements personnels concernés par ce problème de cybersécurité varient en fonction des personnes. D'après nos vérifications, les renseignements personnels vous concernant qui ont pu être affectés par ce problème font partie d'une ou plusieurs des catégories suivantes : votre nom, vos coordonnées (telles que votre numéro de téléphone, votre adresse de courriel et votre adresse postale), votre genre, votre date de naissance, et/ou la date d'anniversaire de votre mariage.
>
> Nous ne croyons pas que les mots de passe, les numéros de compte bancaire ou les informations de carte de paiement aient été affectées par ce problème."

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

44. Accordingly, in the case of Plaintiff and many other Class Members, these Class Members remained uninformed of the Data Breach during over two months after it occurred and remain highly vulnerable to fraud and identity theft. This represents additional faults and gross negligence by Defendant.

45. 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.

46. 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.

47. 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.

48. 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.

49. 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.

50. Defendant's negligently waited to provide its clients with the (limited and inadequate) mytruidentity® credit monitoring plan. This aggravated the risk that their private information would be used by malicious criminals.

51. In addition, considering that the personal and financial information of likely millions of MGM clients have been stolen, it will take much longer that 1 year for the thieve(s) to use and/or sell all of the stolen 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. Defendant is clearly responsible to indemnify and hold the Class Members harmless of all losses and damages suffered well over twelve to twenty-four months since the Data Breach.

52. 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:

53. 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.

54. 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 by unauthorized parties;

b. failed to promptly notify the Plaintiff and the Class Members of the Data Breach for over two months, which in and of itself is abusive;

c. 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;

d. already permitted the theft of personal and/or financial information in the context of the July 2019 MGM data breach mentioned above and it permitted an even more significant data breach to occur only 4 years later, evidencing Defendant's lack of consideration toward the Class Members, some of which are involved in both class actions as mentioned above.

e. permitted very sensitive and private information to be accessed and stolen - as mentioned above, the stolen information included name, contact information (such as phone number, email address, and postal address), gender, date of birth, and driver's license number, Social Security/insurance number, passport number and wedding anniversary date.

f. lied to cover up its faults and downplay the magnitude of this second Data Breach. In this regard, we refer to Defendant's R-3 report filed with the United States Securities and Exchange Commission in which Defendant intentionally misrepresented that it was able to "prevent the criminal actors from accessing any customer bank account numbers or payment card information." However, as mentioned above, in the R-5 email Defendant sent to the Plaintiff, Defendant confirms that "*Nous ne croyons pas que les mots de passe, les numéros de compte bancaire ou les informations de carte de paiement aient été affectées par ce problème*.".

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 telephone hotline number indicated in the R-5 emails only sends calls to TransUnion and not to MGM itself. Furthermore, the TransUnion representatives who answer such calls are not able to confirm what information was actually stolen regarding

the caller / Class Member in question.

i. It only sent the R-5 emails in French, which is not understood by many Canadians (including in Quebec).

j. failed to offer indemnification and proper insurance coverage to Class Members.

k. failed to offer to indemnify the Class Members for their losses.

55. Considering the above and considering the fact that Defendant has repeatedly 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.

56. 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.

57. 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.

58. The Zuckerman vs MGM Resorts International Class Action (R-6) itself further justify the claim for punitive damages in both that file and the present matter, especially for those class members included in both data breach, who are justifiably worried that the new November 2023 notification emails (R-5) are actually fraudulent activity (including social engineering and/or phishing attempts) resulting from the first July 2019 data breach.

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

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

60. Every Class Member had his, her or its sensitive personal and/or financial information lost by Defendant as described hereinabove, including without limitation name, contact information (such as phone number, email address, and postal address), gender, date of birth, and driver's license number, Social Security/insurance number, passport

number, wedding anniversary date, passwords, bank account numbers, credit card number and other payment card numbers, as mentioned above.

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

62. 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.

63. 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.

64. 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.

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

66. 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.

67. 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.

68. Some Class Members are included in both the MGM July 2019 data breach and the most recent September 2023 Data Breach herein.

CONDITIONS REQUIRED TO INSTITUTE A CLASS ACTION

69. 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.

70. 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.

71. 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.

72. 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.

73. 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.

74. 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.

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

76. 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 September 11, 2023?

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?

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

NATURE OF THE ACTION AND CONCLUSIONS SOUGHT

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

79. 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.

80. 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-5 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, which is also the case of Defendant's attorneys in the Zuckerman file mentioned above.

81. 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-5 notification email 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 a result of said loss of information;

c) He will be forced to incur out of pocket expenses in order to further protect himself and his credit file, for which he holds Defendant liable, namely in order to purchase further credit monitoring protection.

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

e) 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;

f) 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;

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;

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.

82. 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 September 11, 2023, 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 September 11, 2023?

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 X (formerly 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, DECEMBER 1, 2023

(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

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 R-1: Nevada Entity Search Business Information online report regarding Defendant.

Exhibit R-2: TechCrunch article entitled "MGM Resorts blames 'cybersecurity issue' for ongoing outage", dated September 11, 2023

Exhibit R-3: Defendant's "Current Report" filed with the United States Securities and Exchange Commission.

Exhibit R-4: Defendant's "Notice of Data Breach" dated October 5, 2023.

Exhibit R-5: November 27, 2023 notification email sent by Defendant to Plaintiff.

Exhibit R-6: August 3, 2022 authorization Judgment in Zuckerman vs. MGM Resorts International, 2022 QCCS 2914.

Exhibit R-7: Online submissions and comments received from multiple Class Members (*en liasse*, under seal and confidentially - without waiving professional secrecy).

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, DECEMBER 1, 2023

(s) Lex Group Inc.

Lex Group Inc.
Per: David Assor
Class Counsel / Attorneys for Plaintiff

NOTICE OF PRESENTATION
(Articles 146 and 574 al. 2 C.P.C.)

TO:

MGM RESORTS INTERNATIONAL
3600 Las Vegas Boulevard South,
Las Vegas, Nevada, U.S.A., 89109

Defendant

TAKE NOTICE that Plaintiff's APPLICATION FOR AUTHORIZATION TO INSTITUTE A CLASS ACTION will be presented before the Superior Court at **1 Rue Notre-Dame E, Montréal, Quebec, H2Y 1B6**, on the date set by the Coordinating Judge of the Class Action Division.

DO GOVERN YOURSELVES ACCORDINGLY.

MONTREAL, DECEMBER 1, 2023

(s) Lex Group Inc.

Lex Group Inc.
Per: David Assor
Class Counsel / Attorneys for Plaintiff