

Matthew E. Yarbrough
100 Crescent Court, Suite 700
Dallas, TX 75201
mey@ylawgroup.com
214.263.7500

September 7, 2019

File No. 44293.9

VIA E-MAIL

Wayne Stenehjem, Attorney General
Office of Attorney General
600 East Boulevard Avenue, Department 125
Bismarck, ND 58505
Email: ndag@nd.gov

I represent MGM Resorts International (“MGM”), a hospitality corporation, with respect to a recent data security incident. MGM is a hotelier headquartered in Las Vegas, Nevada. This letter is submitted on behalf of MGM pursuant to N.D. Cent. Code §§ 51-30-01 *et seq.*, because the personal information of 45,514 North Dakota residents may have been affected by the incident.

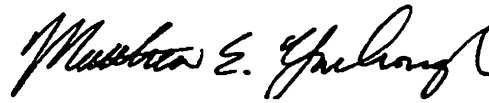
On or about July 7, 2019, an outside unknown individual (“UI”) accessed MGM’s internal system without authorization and exfiltrated data by exploiting a compromised account concerning a third-party integration. On July 10, 2019, the UI posted the data on a closed internet forum with the intent to sell the information for financial gain. The data was taken down from the forum on or about July 24, 2019. Outside legal counsel engaged with two forensic investigation firms to conduct an exhaustive analysis of the compromised data. The vast majority of information contained within the data set included names, addresses, and phone numbers. No MGM customer financial information or passwords were accessed.

On August 9, 2019, after an arduous forensic and time-intensive search of the data set, MGM determined that 45,514 North Dakota residents first and last name in combination with dates of birth were accessed without authorization.

MGM is dedicated to the security, privacy and confidentiality of its customers’ information. Currently, MGM is in the process of notifying affected residents via the attached letter. MGM is offering twelve (12) months of complimentary credit monitoring, identity monitoring, and up to \$1,000,000 of reimbursement insurance to the affected residents through ID Experts. Please contact me should you have any questions.

Office of Attorney General
August 13, 2019
Page 2

Very truly yours,

A handwritten signature in black ink, appearing to read "Matthew E. Yarbrough". The signature is fluid and cursive, with a large, sweeping initial "M".

Matthew E. Yarbrough
214.263.7500

Enclosure: Consumer Notification Letter



MGM RESORTS

MGM Resorts International
 C/O ID Experts
 PO Box 4219
 Everett WA 98204

ENDORSE



4ND NAME
 ADDRESS1
 ADDRESS2
 CSZ

SEQ
 CODE 2D

BREAK

To Enroll, Please Call:
 833-959-1344
 Or Visit:
<https://ide.myidcare.com/mgmri>
 Enrollment Code:
 <<XXXXXXXXXX>>

<<LTR_DATE>>

Notice of Data Incident

Dear <<First Name>> <<Last Name>>,

What Happened

On or about July 7, 2019, an individual accessed MGM Resorts International’s computer network system without permission. The individual downloaded partial customer data from MGM’s computer systems, then posted and disclosed part of the data on a closed internet forum. No customer financial information, passwords or credit cards were part of the data in question and it was taken down and removed from the closed internet site.

What Information Was Involved

MGM immediately initiated an internal forensic investigation into this incident. MGM conducted an exhaustive investigation and search of the downloaded data from the closed internet site. On August 9, 2019, MGM determined your First Name, Last Name, and Date of Birth were part of the compromised file. Again, no financial information, passwords or credit cards were included in the database.

What We Are Doing

We take the security of our customers’ data seriously, and after MGM became aware of the event, we took immediate measures to investigate and remediate the incident. We have implemented additional safeguards to improve further data security related to external software incidents. Furthermore, MGM reported the incident to law enforcement immediately once MGM discovered the matter.

In addition, we are offering identity theft protection services through ID Experts®, a data incident and recovery services expert, to provide you with MyIDCare™. The MyIDCare service includes: twelve (12) months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is possibly compromised.

What You Can Do

We encourage you to contact ID Experts with any questions and to enroll in the free MyIDCare services by calling 833-959-1344 or going to <https://ide.myidcare.com/mgmri> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is <<ENRL_DT>>.

At this time, MGM does not believe that your limited information has been misused. However, we encourage you to take full advantage of this service offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 833-959-1344 or go to <https://ide.myidcare.com/mgmri> for assistance or for any additional questions you may have.

Sincerely,

MGM Resorts International

(Enclosure)



Recommended Steps to help Protect your Information from MyIDCare

- 1. Website and Enrollment.** Go to <https://ide.myidcare.com/mgmri> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.
- 3. Telephone.** Contact MyIDCare at 833-959-1344 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.alerts.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.