

Antony Kim
Direct Dial: +1.202.637.3394
antony.kim@lw.com

555 Eleventh Street, N.W., Suite 1000
Washington, D.C. 20004-1304
Tel: +1.202.637.2200 Fax: +1.202.637.2201
www.lw.com

LATHAM & WATKINS LLP

October 6, 2023

VIA EMAIL

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
consumer@ag.iowa.gov

FIRM / AFFILIATE OFFICES

Austin	Milan
Beijing	Munich
Boston	New York
Brussels	Orange County
Century City	Paris
Chicago	Riyadh
Dubai	San Diego
Düsseldorf	San Francisco
Frankfurt	Seoul
Hamburg	Shanghai
Hong Kong	Silicon Valley
Houston	Singapore
London	Tel Aviv
Los Angeles	Tokyo
Madrid	Washington, D.C.

Re: Notice of Data Security Incident

Dear Attorney General,

I am writing on behalf of Caesars Entertainment, Inc. (the “Company”) to provide you with information about a data security incident impacting residents of your state. On August 19, 2023, the Company identified suspicious activity in its information technology network resulting from a social engineering attack on an outsourced IT support vendor used by the Company. After detecting the suspicious activity, the Company quickly activated its incident response protocols and implemented a series of containment and remediation measures to reinforce the security of its information technology network. The Company also launched an ongoing investigation, engaged leading cybersecurity firms to assist, and notified law enforcement and state gaming regulators. On September 14, 2023, the Company publicly disclosed the incident through a Form 8-K filing.¹

On September 7, 2023, the Company determined that the unauthorized actor acquired a copy of, among other data, its loyalty program database, which includes the driver’s license number, social security number, or other government-issued ID number for a significant number of members in the database. The loyalty program database contains such personal information of approximately 384,087 residents of your state.

The Company will begin notifying individuals affected by this incident consistent with its legal obligations this week and will continue offering two-year credit monitoring and identity protection services for affected individuals (as was originally announced in its Form 8-K filing). A copy of this notice is attached as Appendix A. As part of its ongoing operations and in response to this incident, the Company has deployed advanced security tooling across its network and engaged in tactical security hardening activities, as well as dark web monitoring. The Company has also taken steps to ensure that the specific outsourced IT support vendor involved in this matter


¹ See Caesars Entertainment, Inc., Form 8-K (Sept. 14, 2023), <https://investor.caesars.com/node/33686/html>

LATHAM & WATKINS LLP

has implemented corrective measures to protect against future attacks that could pose a threat to its systems.

If your office requires any further information in regard to this matter, please contact me at (202) 637- 3394 or tony.kim@lw.com.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Antony P. Kim". The signature is written in a cursive, flowing style.

Antony Kim
of LATHAM & WATKINS LLP

Enclosures

Appendix A

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

[Date], 2023

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

We are writing to provide you with information about a cybersecurity incident involving your personal information that Caesars Entertainment, Inc. publicly disclosed through a Form 8-K filing on September 14, 2023. We wanted to share some details and offer you some resources that you may find helpful. Please note the section titled "What You Can Do" below.

What Happened? Caesars Entertainment, Inc. (the "Company," "we," or "our") identified suspicious activity in our information technology network resulting from an attack on an IT support vendor used by the Company. After detecting the suspicious activity, we quickly activated our incident response protocols and implemented a series of containment and remediation measures. The Company also launched an ongoing investigation, engaged leading cybersecurity firms to assist, and notified law enforcement and state gaming regulators. Once the incident was contained, we initiated a detailed review to identify any sensitive personal information contained in data acquired by the unauthorized actor as part of the incident.

What Information is Involved? The incident impacted our loyalty program database. Your information is contained in that database, including, among other data, your name and <<AFFECTED DATA ELEMENTS>>. We have no evidence that any customer passwords/PINs, bank account information, or payment card numbers were affected by the incident.

What Are We Doing? We have taken steps to ensure that the stolen data is deleted by the unauthorized actor, although we cannot guarantee this result. We are monitoring the web and have not seen any evidence that the data has been further shared, published, or otherwise misused. However, to ease any concern you may have, we are offering you complimentary identity theft protection services for two years through IDX, a data breach and recovery services expert. This identity protection service includes two years of credit and dark web monitoring to help detect any misuse of your information, as well as a \$1,000,000 insurance reimbursement policy and fully managed identity restoration in the event that you fall victim to identity theft. To activate these services, you may follow the instructions included in the section below on *Steps You Can Take to Help Protect Your Information*.

What You Can Do. While we do not have any specific reason to believe that you are at risk of identity theft or fraud as a result of this incident, it is always good practice to be vigilant by regularly reviewing your account statements and monitoring any available credit reports for suspicious activity. We also generally encourage you to take care in identifying calls, emails or SMS texts that appear to be spam or fraudulent (e.g., phishing), and to avoid opening links or attachments sent from untrusted sources. You may also review the section below on *Steps You Can Take to Help Protect Your Information* as a helpful resource.

For More Information. For further information, please call 1-888-652-1580, Monday to Friday from 9 am – 9 pm Eastern Time.

Steps You Can Take to Help Protect Your Information

Enroll in IDX Credit Monitoring and Identity Protection Services

Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the [email or letter]. Please note the deadline to enroll is [Date].

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call toll-free 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file with the credit reporting bureau. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

If you discover any suspicious items on your credit reports or from the fraud alert and have enrolled in IDX identity protection, notify them immediately by calling or logging into the IDX 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 the IDX ID Care team, who will help you determine the cause of the suspicious items. In the 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.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report free of charge, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover their information has been misused to file a complaint. You can obtain further information on how to file such a complaint using the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud (this letter alone does not suggest that you are a victim of or at risk of identity theft or fraud). Please note that in order for you to file a police report for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For California residents, the California Office of Privacy Protection (www.oag.ca.gov/privacy) may be contacted for additional information on protection against identity theft. The California Attorney General can be contacted at 1300 I Street, Sacramento, CA 95814, www.oag.ca.gov, 800-952-5225.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 888-743-0023.

For North Carolina residents, the North Carolina Attorney General can be contacted at Mail Service Center 9001, Raleigh, NC 27699, www.ncdoj.gov, 877-566-7226.

For Rhode Island residents, the Rhode Island Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400. You have the right to file or obtain a police report regarding this incident.

For District of Columbia residents, the District of Columbia Attorney General can be contacted at 400 6th Street NW, Washington, DC 20001, www.oag.dc.gov, 202-727-3400.

For Iowa residents, the Iowa Attorney General can be contacted at 1305 E. Walnut Street, Des Moines, Iowa 50319, www.iowaattorneygeneral.gov, 515-281-5926, or 888-777-4590.

For New York residents, the New York Attorney General may be contacted at the Capital, Albany, NY 12224, www.ag.ny.gov, 800-771-7755.

For Oregon residents, the Oregon Attorney General may be reached at 1162 Court Street NE, Salem, OR 97301, www.doj.state.or.us, 503-378-6002.

For South Carolina residents, the South Carolina Department of Consumer Affairs may be reached at 293 Greystone Blvd., Ste. 400, Columbia, SC 29210, www.consumer.sc.gov, 800-922-1594.

For Kentucky residents, the Kentucky Attorney General may be contacted at 700 Capital Avenue, Suite 118, Frankfort, KY 40601, www.ag.ky.gov, 502-696-5300.

For Massachusetts residents, you have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, you have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers;

you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.