

June 25, 2024

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

**Re: AEG Presents, LLC
Data Breach Notification**

To Whom This May Concern,

We, AEG Presents, LLC (“**Company**”) are making this report to the Office of the Maryland Attorney General because we recently learned of a security incident as described further below.

I. Brief Description of the Security Incident

On June 18, 2024, we learned that an employee had emailed certain company files from their work email account to their personal email account between September 27, 2021 and May 3, 2024. Such company files included confidential and proprietary information belonging to the Company, but also included other employees’ name, social security number/tax identification number and HR information, such as email address, original hire date, and job title. The employee is no longer employed by us.

II. Number of Maryland Residents Affected by the Incident

We estimate that 4 Maryland residents have been affected by the incident and will notify these residents on or around June 26, 2024. A sample copy of the notice being sent to the affected residents is separately attached to the cover email.

III. Steps Taken to Remedy the Incident

Upon learning of this event, we immediately worked with forensic experts to identify and contain the data. **A forensic investigation has found no evidence that the data has been downloaded, forwarded, used, or transferred to any other person or location.** The former employee declared that he did not use, disclose, send, save, or transfer the data. We have not found any evidence or indication that any personal data is or was acquired by any unauthorized person or that it is subject to any risk of harm and the former employee assured us that neither is the case. We also immediately took steps to disable certain features of the our system to further restrict access and are working with subject-matter experts to implement other risk mitigation measures. We have also commenced a review on our access control policies and procedures to certain applications.

* * * * *

If you have further questions or concerns, please contact us at Robin.Samuel@bakermckenzie.com.

Sincerely,

AEG Presents, LLC

425 West 11th Street Suite 400 Los Angeles, CA 90015

AEG Presents, LLC
425 West 11th Street, Suite 400
Los Angeles, CA 90015
United States

June 25, 2024

NOTICE OF DATA BREACH

WHAT HAPPENED AND WHAT INFORMATION WAS INVOLVED?

On June 18, 2024, AEG Presents, LLC (“we” or “Company”), learned that an employee had emailed certain company files from their work email account to their personal email account between September 27, 2021 and May 3, 2024. Such company files included confidential and proprietary information belonging to the Company, but also included your name and social security number. This transmission of data was and is against Company policy. The employee is no longer employed by us.

A forensic investigation has found no evidence that the data has been downloaded, forwarded, used, or transferred to any other person or location. The former employee declared that he did not use, disclose, send, save, or transfer the data. We have not found any evidence or indication that any of your personal data is or was acquired by any unauthorized person or that it is subject to any risk of harm and the former employee assured us that neither is the case. The incident therefore does not trigger statutory notification obligations. Nonetheless, we decided to inform you in the interest of transparency and to clarify that we do not tolerate breaches of Company policies.

WHAT WE ARE DOING

Upon learning of this event, we immediately worked with forensic experts to identify and contain the data. We also immediately took steps to disable certain features of our system to further restrict access. We have also commenced a review on our access control policies and procedures to certain applications. We have been in contact with personnel and other stakeholders about how we are responding to the incident. We are also scanning the dark web for any indications that the data has been subject to unauthorized access.

WHAT YOU CAN DO

We encourage you to remain vigilant about any suspicious activity involving your personal data. For example, please do not open attachments or click on links in electronic communications from unknown senders, and please do not reveal personal or confidential information to unknown persons over the phone or other channels. If someone you think you recognize is asking you to take steps outside of your normal work functions, we recommend that you verify their identity before proceeding. If you receive any suspicious requests or communications, please report them to the IT help desk and wait for further instructions.

OTHER IMPORTANT INFORMATION

Please consider the following additional information:

- You may wish to visit the website of the U.S. Federal Trade Commission at <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> or reach the FTC at 877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC.

- You may have the right to obtain any police report filed related to this incident, and to file a police report and obtain a copy of it if you are the victim of identity theft.
- U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free 877-322-8228.
- If you are a North Carolina resident, you can find more information on how to prevent identity theft through this official North Carolina Attorney General website: <https://ncdoj.gov/protecting-consumers/identity-theft/>. You can contact the North Carolina Attorney General's Office using the following contact details:

North Carolina Attorney General's Office
 Consumer Protection Division
 9001 Mail Service Center
 Raleigh, NC 27699-9001
 877-566-7226 (Toll-free within North Carolina)
 919-716-6000
www.ncdoj.gov

- If you are a Maryland resident, you can contact the Maryland Attorney General's Office using the following contact details:

Office of the Attorney General
 200 St. Paul Place
 Baltimore, MD 21202
 1-888-743-0023 (Toll-free within Maryland)
<https://www.marylandattorneygeneral.gov/>

- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus listed below. At no charge, if you are a U.S. resident, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit, mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies and you may be required to provide information such as your: (1) name; (2) Social Security number; (3) date of birth; (4) current address; (5) addresses over the past five years; (6) proof of current address; (7) copy of government identification; and (8) any police/investigative report or complaint. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.
 - Experian: 888-397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013
 - Equifax: 800-525-6285; www.equifax.com; P.O. Box 105788, Atlanta, GA 30348
 - TransUnion: 800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000

- You have relevant rights pursuant to the federal Fair Credit Reporting Act. For more information, please see the U.S. Federal Trade Commission's bulletin on Fair Credit Reporting Act rights available here: <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

To help relieve concerns and restore confidence following this incident, we have secured the services of IDX, A ZeroFox Company, to provide identity monitoring at no cost to you for two years if you choose to register and activate the services. The identity monitoring services available to you include credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. To activate your identity monitoring services and for additional details, please scan the QR code below or visit: <https://app.idx.us/account-creation/protect>. You will need to reference the enrollment code listed below when calling or enrolling online, so please do not discard this letter. You have up to 120 days to activate the identity monitoring services.

Enrollment Code: << [REDACTED] >>

To Enroll, Scan the QR Code Below:




Or Visit:

<https://app.idx.us/account-creation/protect>

FOR MORE INFORMATION

If you have further questions or concerns, please contact us at [REDACTED], or call us at [REDACTED].

Sincerely,

AEG Presents, LLC