MAYNARD
COOPER GALE

Adam Griffin
DIRECT 205.415.4903
EMAIL AGriffin@maynardcooper.com

March 2, 2023

Attorney General Anthony G. Brown
Office of Attorney General
Attn: Security Breach Notification
Baltimore, MD 21202

Re: Notice of a Security Incident

Dear Attorney General Brown,

I am writing to let you know that our client, Cineplex Entertainment LP ("Cineplex" or "Company"), experienced a security incident that affected the personally identifiable information of some current and former employees and their dependents, including four (4) individuals in Maryland. We are providing notice to your office pursuant to Md. Code Ann. Comm. Law 14-3504.

On February 6, 2023, Cineplex discovered that personal information of its employees and their dependents may have been accessed by an unauthorized third party in connection with a data security incident experienced by one of its third-party vendors, Fortra, LLC ("Fortra"). Fortra operates a data transfer platform that Cineplex uses to provide accurate and up-to-date information to payroll service providers. Fortra determined that an unknown third party accessed Fortra's data transfer platform, GoAnywhere, between January 28, 2023 and January 30, 2023. On February 7, 2023, Fortra notified Cineplex that its own internal investigation determined that Cineplex data was indeed subject to unauthorized acquisition.

Thereafter, Cineplex reviewed information provided by Fortra to determine what specific sensitive information was involved and to whom it related. Following the conclusion of this review, Cineplex provided written notice of this incident to all affected individuals on March 2, 2023. A representative example of the notice furnished to these individuals is enclosed as **Exhibit A**. These individuals were offered complimentary credit monitoring and identity protection services through TransUnion for twenty-four (24) months. Cineplex is not aware of any actual or attempted misuse of personal information as a result of this incident.

The information that could have been subject to unauthorized access includes the names, date of birth, Social Security numbers, and financial account information of current and former employees and their dependents.

As part of the ongoing commitment to the security of information in its care, Cineplex is reviewing existing policies and procedures that govern third-party vendors and evaluating additional measures and safeguards to protect against this type of incident in the future. Moreover, Fortra indicated it notified law enforcement of this incident. Cineplex is also providing impacted individuals with guidance on how to better protect against identity theft, fraud, and information on how to place a fraud alert and security freeze on one's credit file. The notice to impacted individuals also included the contact details for the national consumer reporting agencies and the Federal Trade Commission.

Please do not hesitate to let me know if you have any questions.

Very truly yours,

EXHIBIT A

1303 Yonge St
Toronto ON M4T 2Y9

March 2, 2023

000001

John Sample
123 Street
City ST 12345
United States of America

RE: **Notice of Data Breach**

Dear John Sample,

Cineplex Entertainment LP ("Cineplex") is writing to inform you of a recent incident at one of our third-party vendors that may affect the privacy of some of your personal information, and to provide you with the information required to enroll in the TransUnion Credit Monitoring service.

We are not aware of any actual or attempted misuse of your personal information as a result of this incident. However, we want to make sure that you are aware of what happened, our response, and resources available to you to help protect your information from misuse, should you feel it necessary to do so.

You may have already received electronic notification about this matter. If so, this pertains to the same incident.

What Happened?

On Monday, February 6, 2023, Cineplex learned that a third-party vendor we use suffered a data security incident. On January 30, 2023, this third-party vendor discovered it was the target of a cyber incident. The vendor operates a data transfer platform that Cineplex uses to provide accurate and up-to-date information to payroll service providers. Cineplex itself was not the target of this incident and did not experience any internal compromise of data.

Upon learning of the incident, Cineplex commenced an immediate investigation to determine what, if any, sensitive Cineplex data was potentially involved. The investigation included working diligently to gather further information from the vendor to understand the scope of the incident. We have no indication at this time that any personal information has been misused as a result of this event.

What Information is Involved?

While we are still working to determine the full scope of the personal information that has been compromised for employees and their dependents, the information related to you that may have been impacted includes your name, date of birth, Social Security Number, and financial account information.

What Are We Doing?

We take the security of information entrusted to us various seriously and apologize for the inconvenience this incident has caused. We are taking steps to protect all Cineplex employees and their dependents by delivering this notification and providing immediate access to credit monitoring services. We assure you that Cineplex takes the protection of the information of our employees, former employees and their dependents very seriously and that we are taking all necessary steps to prevent a similar incident from reoccurring. We are also notifying state regulators, where required.

What You Can Do

As a best practice, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and credit reports for suspicious activity. You may also review the enclosed information. Although we are not aware of any actual or attempted misuse of your personal information, as an added precaution we have arranged to offer you access to twenty-four months of complimentary credit monitoring and identity protection services provided through TransUnion. Although we are making these services available to you, we are unable to enroll you directly. For enrollment instructions, please review the enclosed information.

For More Information

We understand that you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, we established a dedicated email address at **cineplexprivacy@cineplex.com.**

We appreciate the sensitivity of your information and acknowledge how unsettling this incident is and the inconvenience it has caused. On behalf of the Cineplex Executive Leadership Team, I can assure you that we are doing everything we can to protect our employees and ensure this does not happen again.

Sincerely,

Thomas Santram
SVP, General Counsel
Cineplex Entertainment LP

IDENTITY PROTECTION REFERENCE GUIDE

1. Online Monitoring Services. We have retained the assistance of Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

Through Cyberscout, we have arranged a **two year** subscription to an online monitoring service, at no cost to you. This credit monitoring service will notify you by email of critical changes to your Credit Report. Should you receive an email alert, you can review and validate the reported change by logging into the portal. This allows you to identify any potentially fraudulent activity on your Credit Report.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit:

https://secure.identityforce.com/benefit/Cineplex

You will be prompted to enter the following activation code:

1AB2C3D4

Please ensure that you redeem your activation code before June 30, 2023, to take advantage of the service.

Upon completion of the enrollment process, you will have access to the following features:

- ✓ Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- ✓ Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- ✓ Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.
- ✓ Identity theft insurance of up to $1,000,000 in coverage to protect against potential damages related to identity theft and fraud
- ✓ Assistance with reading and interpreting credit reports for any possible fraud indicators.
- ✓ Assistance with answering any questions individuals may have about fraud.

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-877-694-3367.

2. Review your Credit Reports. We recommend that you monitor your credit reports for any activity you do not recognize. Under federal law, you are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To order your free annual credit report, visit **www.annualcreditreport.com**, call toll-free (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at **www.ftc.gov** and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

3. Place Fraud Alerts. 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. Please note that placing a fraud alert may delay you when seeking to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-806-1627
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

It is only necessary to contact 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 should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

4. Place Security Freezes. By placing a security freeze, someone who fraudulently acquires your personally identifying information will not be able to use that information to open new accounts or borrow money in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security 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.

To place a security freeze, you must contact each of the three national credit reporting bureaus listed above and provide the following information: (1) your full name; (2) your social security number; (3) date of birth; (4) the addresses where you have lived over the past two years; (5) proof of current address, such as a utility bill or telephone bill; (6) a copy of a government issued identification card; and (7) if you are the victim of identity theft, include the police report, investigative report, or complaint to a law enforcement agency. If the request to place a security freeze is made by toll-free telephone or secure electronic means, the credit bureaus have one business day after receiving your request to place the security freeze on your credit report. If the request is made by mail, the credit bureaus have three business days to place the security freeze on your credit report after receiving your request. The credit bureaus must send confirmation to you within five business days and provide you with information concerning the process by which you may remove or lift the security freeze.

5. Monitor Your Account Statements. We encourage you to carefully monitor your financial account statements, medical provider statements, and insurance statements for fraudulent activity and report anything suspicious to the respective institution or provider.

6. You can obtain additional information about the steps you can take to avoid identity theft and more information about fraud alerts and security freezes from the FTC. You may contact the FTC, Consumer Response Center at: 600 Pennsylvania Avenue NW, Washington, DC 20580, **https://www.identitytheft.gov/#/**, 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502.

****

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and **oag@dc.gov**.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and **www.oag.state.md.us**.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and **www.ncdoj.gov**.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; **www.riag.ri.gov**; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island residents impacted by this incident.

F*or New Mexico residents,* 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 bureaus 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 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. We encourage you to 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or **https://ag.ny.gov/**.