Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 24-024

Investigation by LETITIA JAMES,
Attorney General of the State of New York, of

NATIONAL AMUSEMENTS, INC.,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York ("OAG") commenced an investigation pursuant to, *inter alia*, Executive Law § 63(12) and General Business Law ("GBL") §§ 899-aa and 899-bb into a data security incident at National Amusements, Inc. ("National" or "Respondent"). This Assurance of Discontinuance ("Assurance") contains the findings of OAG's investigation and the relief agreed to by OAG and National (collectively, the "Parties"), whether acting through its respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries.

OAG FINDINGS

1. National is one of the nation's largest privately controlled movie theater operators. National operates 759 cinemas screens throughout the United States, the United Kingdom and Latin America.

2. On December 15, 2022, National first received an alert of suspicious activity on its network from a managed service provider. National utilized Sentinel One, an endpoint detection monitoring system, which alerted and showed National's performance monitoring systems were

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

going offline, possible exfiltration activity occurring and malware presence in the system.

3. Upon receiving the alert, National immediately disconnected internet access to all networks, including the payment card network. A preliminary investigation found that the suspicious activity was localized in the corporate network. National reset users' password for all domains. CrowdStrike Falcon was implemented across the network.

4. From December 15, 2022 to March 3, 2023, National undertook a forensic investigation. National also reported the incident to the Federal Bureau of Investigation on December 16, 2022. The investigation determined the attacker accessed the network on December 13, 2022. The threat actor used an employee's VPN credentials, most likely obtained from the dark web, to enter the network. National had multifactor authentication in place for remote access prior to the incident. However, National's single virtual private network ("VPN"), which was not intended for general use, did not have multifactor authentication. The VPN tunnel was closed immediately after the incident.

5. Once in the network, the threat actor utilized Cobalt Strike to extract additional credentials in order to gain additional network privileges.

6. Information exposed by this breach included name, date of birth, social security number, passport number, financial account number, driver's license number and health insurance number. National maintains that no consumers or patrons were impacted by this breach and the information was of former and current employees and contractors.

7. In response to the incident, National engaged a third-party forensic cybersecurity firm to remediate and restore National's systems. The forensic firm found software in the environment which can be used to exfiltrate documents. Additionally, the threat actor provided a file tree of information taken from the company.

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

8. A small portion of the network contained a subset of social security numbers that were not encrypted. In fact, National's IT team was unaware that certain unencrypted data was stored on the network.

9. From March 3, 2023 to August 23, 2023, National reviewed 55.6 gigabytes of data to determine the names and contact information of victims that were impacted by this data breach. The review completed around November 2, 2023 and notification to the individuals didn't take place until December 18, 2023, over one year after the incident occurred.

10. The breach affected a total of 82,128 individuals, of which 23,365 were New York residents.

11. The OAG's investigation identified the following areas where National failed to implement reasonable data security practices:

a. Encryption: National failed to encrypt social security numbers and other private information on a portion of its network.

b. Multi-Factor Authentication: National failed to employ multi-factor authentication across one access point at the time of the incident.

c. Data Security Assessments: National's data security assessments did not identify the vulnerability described above.

d. Password Rotation: National did not enforce its password complexity and rotation requirements as to a portal that was the subject of the incident.

12. Based on the foregoing, the OAG has concluded that National violated Executive Law § 63(12) and GBL §§ 899-aa, and 899-bb.

13. Respondent neither admits nor denies OAG's Findings, paragraphs 1-12 above.

14. The OAG finds the relief and agreements contained in this Assurance appropriate

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

and in the public interest. THEREFORE, the OAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12), and GBL §§ 899-aa, and 899-bb.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

PROSPECTIVE RELIEF

15. For the purposes of this Assurance, the following definitions shall apply:

    a. "**Effective Date**" shall be the date of the last signature to this Agreement.

    b. "**Company Employee**" means any New York resident who is a current or former employee or contractor of National.

    c. "**Company Private Information**" means Private Information (as defined by GBL § 899-aa(1)(b)) that National collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes relating to Company Employees or relating to New York residents that purchase goods or services from National.

    d. "**Compensating Controls**" shall mean alternative mechanisms that are put in place to satisfy the requirement for a security measure that is determined by the Chief Information Security Officer or his or her designee to be impractical or unreasonable to implement at the applicable time due to legitimate technical or business constraints. Such alternative mechanisms must: (a) meet the intent and rigor of the original stated requirement; (b) provide a similar level of security as the original stated requirement; (c) be materially and substantively up-to-date with current industry accepted security protocols; and (d) be commensurate with the additional risk imposed by not adhering to the original stated

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

requirement. The determination to implement such alternative mechanisms must be accompanied by written documentation demonstrating that a risk analysis was performed indicating the gap between the original security measure and the proposed alternative measure, that the risk was determined to be acceptable, and that the Chief Information Security Officer or his or her designee agrees with both the risk analysis and the determination that the risk is acceptable.

16. National shall comply with Executive Law § 63(12), GBL §§ 899-aa, and 899-bb, in connection with its collection, use, and maintenance of Company Private Information, and shall maintain reasonable security policies and procedures designed to safeguard Company Private Information from unauthorized use or disclosure.

17. National shall not misrepresent the extent to which National maintains and protects the privacy, security, confidentiality, or integrity of Company Private Information collected from or about customers.

18. For the avoidance of doubt, this Assurance is binding on the Parties, and nothing herein shall be deemed to bind any affiliates or owners of Respondent, except to the extent that Respondent is deemed to be acting through its affiliates or owners.

19. National shall ensure that the Information Security Program, Specific Information Security Requirements and Incident Response procedures specified at paragraphs 20-28, below, are developed and implemented within 90 days after the Effective Date of this Assurance. For any requirements not fully developed within 90 days, National must implement Compensating Controls.

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

INFORMATION SECURITY PROGRAM

20. Respondent shall maintain a comprehensive information security program that is reasonably designed to protect the security, integrity, and confidentiality of Company Private Information ("Information Security Program"). Respondent shall document in writing the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, include all of the requirements detailed in paragraphs 23-28 and the following processes:

a. Regularly assess, update, and document internal and external risks to the security, integrity and confidentiality of Company Private Information, including but not limited to all entries in the most recent Data Inventory;

b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks Respondent identified with respect to the protection of Company Private Information that are appropriate to: (i) the size and complexity of Respondent's operations; (ii) the nature and scope of Respondent's activities; and (iii) the volume and sensitivity of the Company Private Information that Respondent collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes;

c. Regularly assess and document the sufficiency of any safeguards put in place by or on behalf of National to address the internal and external risks to Company Private Information Respondent identified, and modify the Information Security Program based on the results to ensure that such safeguards comply with this Assurance;

d. Regularly test and monitor the effectiveness of such safeguards and modify the Information Security Program based on the results to ensure the safeguards comply

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

with this Assurance;

e. Regularly assess and document the Information Security Program and adjust the Program in light of changes to Respondent's operations or business arrangements that may have an impact on the effectiveness of the Information Security Program, or any other circumstances that Respondent knows may have an impact on the effectiveness of the Information Security Program; and

f. With respect to service providers that will have access to Company Private Information, take reasonable steps to select service providers capable of reasonably safeguarding Company Private Information, and with respect to service providers that Respondent engages after the Effective Date, contractually require such service providers to implement and maintain reasonable safeguards to protect Company Private Information, and take reasonable steps to verify such service providers are complying with the contractual requirements.

21. Respondent shall designate a qualified employee responsible for implementing, maintaining, assessing, updating, and monitoring the Information Security Program. The designated employee shall have the credentials, background, and expertise in information security appropriate to the level, size, and complexity of their role in implementing, maintaining, assessing, updating, and monitoring the Information Security Program. The designated employee shall report regularly to Respondent's senior management, which may include the Chief Executive Officer or Executive Vice President, or similar roles, concerning Respondent's Information Security Program.

22. Respondent shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, assessing, updating, or

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

monitoring the Information Security Program and shall implement appropriate training of such employees. The notice and training required under this paragraph shall be provided to the appropriate employees within ninety (90) days of the Effective Date of this Assurance, or within sixty (60) days of when an employee first assumes new responsibility for implementing, maintaining, assessing, updating, or monitoring the Information Security Program. Respondent shall document that it has provided the notices and training required in this paragraph.

SPECIFIC INFORMATION SECURITY REQUIREMENTS

23. The Specific Information Security Requirements set forth in this section shall apply to Respondent's information systems, processes and technologies that protect Company Private Information.

24. Data Inventory: Within one hundred eighty (180) days of the Effective Date of this Assurance, to the extent it has not already done so, National must reasonably know the location of Company Private Information. National may achieve the objective through the use of diagrams, procedures, information classification policies, asset scanning or other means.

25. Encryption: National will encrypt Company Private Information that it collects, stores, transmits and/or maintains, whether stored within the National computer network, or transmitted electronically within or outside the network, using a reasonable encryption algorithm.

26. Password Management: National shall maintain reasonable password policies and procedures regarding access to Company Private Information requiring the use of complex passwords, password rotation and ensuring that stored passwords are properly protected from unauthorized access.

27. Authentication Policy and Procedures: National shall maintain reasonable account management and authentication regarding protection of Company Private Information, including

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

forbidding the use of shared user accounts-and requiring the use of multi-factor authentication as reasonably determined by National, e.g., for all administrative or remote access accounts.

28. Penetration Testing: National shall maintain a reasonable penetration testing program designed to identify, assess, and remediate security vulnerabilities within the National computer network regarding the protection of Company Private Information. This program shall include regular penetration testing, risk-based vulnerability ratings, and vulnerability remediation practices that are consistent with industry standards.

INCIDENT RESPONSE

29. Respondent shall establish, implement, and maintain a comprehensive incident response plan in relation to Company Private Information in the possession or control of Respondent. The incident response plan shall be documented in writing and include procedures that align with the requirements of Executive Law § 63(12) and GBL §§ 899-aa and 899-bb, including the following:

a. If Respondent has reason to believe that there has been unauthorized access to or the acquisition of Company Private Information owned, licensed, or maintained by the Respondent (a "Security Event"), Respondent shall promptly conduct a reasonable investigation to determine, at a minimum, whether Company Private Information was accessed or acquired without authorization, and, if so, what Company Private Information was accessed or acquired.

b. If Respondent determines Company Private Information has been, or is reasonably likely to have been, accessed or acquired without authorization, Respondent shall expediently provide each consumer whose Company Private Information has been, or is reasonably believed to have been, accessed or acquired

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

without authorization, by email or letter or other legally valid forms of substitute notice established under New York law, material information concerning the security event that is reasonably individualized to the customer including, at a minimum, the timing of the security event, whether the Company Private Information was accessed or acquired without authorization, what Company Private Information was accessed or acquired, and what actions have been taken to protect the consumer.

INFORMATION SECURITY PROGRAM ASSESSMENTS

30. Within one (1) year of the effective date of this Assurance, Respondent shall obtain a comprehensive assessment of the Information Security Program conducted by an independent third-party assessor who uses procedures and standards generally accepted in the profession which shall be documented (a "Third-Party Assessment Report"). Annually for five (5) years thereafter, Respondent shall obtain Third-Party Assessment Report which Respondent shall maintain for seven (7) years from the date of each Third-Party Assessment Report. The Third-Party Assessment Reports shall:

a. Identify the specific administrative, technical, and physical safeguards maintained by Respondent's Information Security Program;

b. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by Respondent meet the requirements of the Information Security Program and the Assurance and/or whether Compensating Controls are in place.

MONETARY RELIEF

31. National shall pay to the State of New York Two Hundred Fifty Thousand dollars

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

($250,000) in penalties, disgorgement, and costs (the "Monetary Relief Amount"). Payment shall be made payable to the State of New York in full within sixty (60) days of the Effective Date of this Assurance. Any payment shall reference AOD No. 20-024

MISCELLANEOUS

32. Respondent expressly agrees and acknowledges that OAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 38, and agrees and acknowledges that in the event the Assurance is voided:

a. any statute of limitations or other time-related defenses are tolled from and after the Effective Date of this Assurance;

b. the OAG may use statements, documents or other materials produced or provided by Respondent prior to or after the Effective Date of this Assurance;

c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue; and

d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

33. If a court of competent jurisdiction determines that Respondent has violated the Assurance, Respondent shall pay to the OAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

34. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of Respondent, itself. Respondent shall include in any such

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of the OAG.

35. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

36. Any failure by the OAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the OAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by Respondent.

37. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 24-024, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to Respondent, to:

Julie Heinzelman
Associate General Counsel
National Amusements, Inc.
846 University Avenue
Norwood, Massachusetts 02062
D: 781.349.4290 | F: 781.461.1412

If to OAG, to:

Bureau Chief
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005

38. OAG has agreed to the terms of this Assurance based on, among other things, the

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

representations made to OAG by Respondent and its counsel and OAG's own factual investigation as set forth in OAG's Findings, paragraphs 1-12 above. Respondent represents and warrants that neither it nor its counsel has made any material misrepresentations to OAG. If any material misrepresentations by Respondent or its counsel are later found to have been made by OAG, this Assurance is voidable by OAG in its sole discretion.

39. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondent in agreeing to this Assurance.

40. This Assurance is not intended for use by any third party in any other proceeding.

41. Respondent represents and warrants, through the signature below, that the terms and conditions of this Assurance are duly approved.

42. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

43. Nothing contained herein shall be construed to limit the remedies available to OAG in the event that Respondent violates the Assurance after its Effective Date.

44. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

45. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of OAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

46. Respondent acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

47. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

48. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

49. This Assurance may be executed in multiple counterparts by the Parties hereto. All counterparts so executed shall constitute one agreement binding upon all Parties, notwithstanding that all Parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the Effective Date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals.

Docusign Envelope ID: 3696A10E-1D5F-419C-8A28-20372BF316D7

WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance have been affixed hereto on the dates set forth below.

LETITIA JAMES **ATTORNEY GENERAL OF THE STATE OF NEW YORK** By: _____ Clark Russell Deputy Bureau Chief Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005 ____11/13/2024_____ Date	**NATIONAL AMUSEMENTS, INC.** By: DocuSigned by: Paula J. Keough 5B17FBD3022145D... Vice President National Amusements, Inc. 846 University Avenue Norwood, Massachusetts 02062 10/22/2024 _____ Date