Subject: Fandango – Notice of Security Incident

[ATTENTION: EXTERNAL SENDER]

Re: Notice of Data Breach

Hello,

Fandango Media, LLC ("Fandango" or "we") recently detected a security incident. Some of your information may have been impacted in this incident. Please read this notice carefully, as it provides information on what happened and what we are doing in response.

What happened?

We recently became aware of an issue involving Fandango's ticketing checkout page. We promptly investigated the issue with the help of outside cybersecurity specialists, and resolved the issue. Our investigation identified evidence that an unauthorized party could access payment card information associated with certain transactions on our checkout page from October 8-11, 2026. Fandango determined on October 30, 2026 that your information may have been impacted in this incident.

What information was involved?

The information about you that may have been impacted was: payment card number; CVV; expiration date; billing zip; and your email address.

Other categories of information that were **NOT** involved include without limitation:

- your first and last name;
- any government issued identification information;
- Social Security Numbers; and
- Other account information.

What are we doing?

Following detection of the incident, Fandango promptly resolved the issue, investigated with cybersecurity specialists, and further enhanced our processes and protections.

Fandango is offering, free of charge, 24 months of credit monitoring services from IDX, including 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. To take advantage of these services that we are providing free to you, please follow the instructions in Exhibit A and activate by February 13, 2027.

What can you do?

Fandango is not currently aware of any fraudulent use of your information as a result of this incident, but nonetheless is informing customers to take appropriate steps to protect their information. It is always advisable to remain vigilant against attempts at identity theft or fraud, which includes reviewing credit reports and financial accounts for suspicious activity. If you identify suspicious activity, promptly report any unauthorized transactions to your card issuer or bank. Additional information about how to help protect your information is contained in Exhibit B.

For more information

We are committed to protecting the information entrusted to us. If you have any questions regarding this incident or the services available, please contact the call center at 1-866-200-0940 Monday through Friday from 6 am to 6 pm Pacific Time, excluding US holidays.

Sincerely,
Fandango

Exhibit A: Credit Monitoring Enrollment Instructions

1. Website and Enrollment. Go to https://app.idx.us/account-creation/protect or call 1-866-200-0940 and follow the instructions for enrollment using your Enrollment Code, which is: [redacted]

2. Activate the credit monitoring provided as part of your IDX identity protection 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, IDX will be able to assist you.

IDX identity protection services will include two years of the following service components:

- **SINGLE BUREAU CREDIT MONITORING** (adults) - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.
- **CYBERSCAN**™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.
- **IDENTITY THEFT INSURANCE** - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.
- **FULLY-MANAGED IDENTITY RECOVERY** - IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

Exhibit B: Other Important Information

Below are additional helpful tips you may want to consider to help protect your personal information.

Review Your Credit Reports and Account Statements; Report Incidents

It is always advisable to remain vigilant against attempts at identity theft or fraud, including by reviewing your free credit reports and account statements closely for signs of suspicious activity. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to the proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact your local police or law enforcement, the Federal Trade Commission ("FTC"), and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. The FTC's contact details are provided below.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW Washington, DC 20580
http://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)
1-877-FTC-HELP (382-4357

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/requestReport/landingPage.action. Credit reporting agency contact details are provided below.

Equifax
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
www.equifax.com/personal/credit-report-services
800-685-1111

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
www.experian.com/help
888-397-3742

TransUnion
P.O. Box 1000
Chester, PA 19016
www.transunion.com
www.transunion.com/credit-help
888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You have the option to place a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. You may also obtain information about fraud alerts from the FTC.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill. For more information about requesting a security freeze, you may contact the credit reporting agency at the contact information provided above. You may also obtain information about security freezes from the FTC.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act ("FCRA") is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; 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 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 violators. Identity theft victims and active-duty military personnel have additional rights pursuant to the FCRA.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 130, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

Additional Information

If you are the victim of fraud or identity theft, you have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400 for more information about steps you can take to help avoid identity theft.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E Walnut St, Des Moines, IA 50319, 515-281-5926 or 1-888-777-4590, https://www.iowaattorneygeneral.gov/.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul

Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023 for more information about steps you can take to help avoid identity theft.

For Massachusetts residents: You have the right to obtain a police report and request a security freeze as described above.

For New York residents: You can contact the New York Department of State Division of Consumer Protection, 99 Washington Avenue, Albany, NY 12231, http://www.dos.ny.gov/consumerprotection,1-800-697-1220 or the New York Attorney General, The Capitol, Albany, NY 12224, http://www.ag.ny.gov/,1-800-771-7755 for information about steps you can take to help avoid identity theft.

For New Mexico Residents: You have rights pursuant to the FCRA, as described above. You may have additional rights under the FCRA not summarized here. We encourage you to review your rights pursuant to the FCRA by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by contacting the FTC at the contact information listed above.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226 for information about steps you can take to help avoid identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the FTC and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Commercial Services website at https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/.

For Rhode Island residents: You can contact the Rhode Island Attorney General,150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400. You have the right to obtain a police report and request a security freeze as described above.

This email was sent by IDX.

4145 SW Watson Ave, Suite 400 • Beaverton, OR, 97005

Manage Preferences | Privacy Policy | Terms & Conditions

