

PAUL HASTINGS

1 (202) 551-1965
sherresesmith@paulhastings.com

June 27, 2024

VIA OVERNIGHT DELIVERY

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

Re: Incident Notification

Dear Attorney General Brown:

We are writing on behalf of Ticketmaster LLC ("Ticketmaster"), to provide notice regarding a data security incident which may involve the personal information of certain Maryland residents, pursuant to Md. Code, Com. Law § 14-3504(h)(1). By providing this notice, Ticketmaster does not waive any rights or defenses regarding the applicability of Maryland law.

On May 20, 2024, Ticketmaster identified unauthorized activity within a third-party cloud database environment containing Ticketmaster data. In response, Ticketmaster immediately launched an investigation and engaged industry-leading cybersecurity forensic investigators to determine the nature and scope of the activity. On May 23, 2024, Ticketmaster reached the preliminary conclusion that an unidentified third party, without authorization, likely accessed and may have obtained certain information relating to Maryland residents from the third-party cloud database between April 2, 2024, and May 18, 2024. Ticketmaster continues to investigate but anticipates that depending on the individual, the information subject to unauthorized access may include names and contact information. Payment card information such as hashed and/or masked card numbers, the terminal digits of card numbers, card type and, in some cases, expiration date may also have been impacted. Additionally, passport numbers may have been impacted for a limited number of individuals. Ticketmaster's investigation is ongoing and it is not yet clear the extent to which there is actual risk of harm to individuals.

Ticketmaster has contacted and is cooperating with US federal law enforcement authorities regarding this incident, and continues to work with industry-leading cybersecurity forensic investigators to determine the nature and scope of the activity, and any potential impact to data subjects. As part of its efforts, it continues to take technical and administrative steps to further enhance the security of its infrastructure to help detect and prevent further threat actor activity. These measures include rotating passwords for all user and service accounts associated with the affected cloud database, reviewing access permissions, and increased alerting mechanisms deployed in the environment.

Notice of this incident will be provided to relevant individuals, including, out of an abundance of caution, to individuals potentially impacted by the exposure of hashed and/or masked credit card numbers, despite it not being clear whether there is any actual risk of harm to individuals yet. At present, Ticketmaster believes at least one Maryland resident will be notified; however, Ticketmaster's investigation is ongoing. Ticketmaster is in the process of notifying relevant individuals. Notices to individuals in Maryland will be



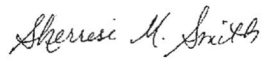
PAUL
HASTINGS

June 27, 2024
Page 2

provided electronically in substantially the same form as the template attached to this correspondence, and will include an offer of one year of identity monitoring at no cost to the individual as a precautionary measure.

If you have any questions regarding the foregoing, please contact me at 1 (202) 551-1965, or by email at sherresesmith@paulhastings.com.

Sincerely,



Sherrese M. Smith
for PAUL HASTINGS LLP

Enclosure

NOTICE OF DATA BREACH

Hello,

We are writing to notify you of a data security incident that may have involved your personal information. We take the protection of your personal information very seriously and are sending this correspondence to tell you what happened, what information was involved, what we have done, and what you can do to address this situation.

What Happened

Ticketmaster recently discovered that an unauthorized third party obtained information from a cloud database hosted by a third-party data services provider. Based on our investigation, we determined that the unauthorized activity occurred between April 2, 2024, and May 18, 2024. On May 23, 2024, we determined that some of your personal information may have been affected by the incident. We have not seen any additional unauthorized activity in the cloud database since we began our investigation.

What Information Was Involved

The personal information that may have been obtained by the third party may have included your name, basic contact information, and «Extra1».

What We Are Doing

We have been diligently investigating this incident with the assistance of outside experts. We have also contacted and are cooperating with federal law enforcement authorities, and this notice has not been delayed due to law enforcement investigation. We have additionally taken a number of technical and administrative steps to further enhance the security of our systems and customer data. These measures include rotating passwords for all accounts associated with the affected cloud database, reviewing access permissions, and increased alerting mechanisms deployed in the environment.

What You Can Do

As described in the enclosed document titled “Additional Resources,” we recommend you remain vigilant and take steps to protect against identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for signs of suspicious activity. To further protect your identity and as a precaution, we are also offering you identity monitoring with TransUnion at no cost to you. Identity monitoring will look out for your personal data on the dark web and provide you with alerts for 1 year from the date of enrollment if your personally identifiable information is found online. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

You can sign up for this service by clicking the following link: <https://bit.ly/TU-sign-up>

Your Ticketmaster account was not affected by this incident, however we recommend being mindful of phishing attempts such as emails from unknown senders or those that contain unusual content, such as links or attachments, or being asked to provide personal information over the phone.

For More Information

We are fully committed to protecting your information, and deeply regret that this incident occurred. If you have questions or concerns regarding this incident, please contact us at 1-800-653-1840 Monday-Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding holidays.

Sincerely,

Ticketmaster

ADDITIONAL RESOURCES

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies (see the "Important Contacts" section for contact details).

You should remain vigilant for incidents of fraud or identity theft by reviewing account statements and monitoring free credit reports. When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. You should also call your local police department and file a report of identity theft. Finally, you should make sure to keep a copy of the police report in case you need to provide it to creditors or credit reporting agencies when accessing or disputing inaccurate information.

You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information about you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain 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 credit freeze, please contact all three major consumer reporting agencies (see the "Important Contacts" section for contact details).

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- Full name, with middle initial and any suffixes;
- Social Security number;
- Date of birth (month, day, and year);
- Current address and previous addresses for the past five (5) years;
- Proof of current address, such as a current utility bill or telephone bill;
- Other personal information as required by the applicable credit reporting agency.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts one year and is placed on a consumer's credit file. 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 credit reporting agencies listed below. The agency you contact will then contact the other two credit agencies.

Important Contacts

To access your credit report, or to implement a security freeze or a fraud alert, you may contact the three major credit reporting agencies listed below.

	Access your Credit Report	Implement a Security / Credit Freeze	Implement a Fraud Alert
Equifax	P.O. Box 740241 Atlanta, GA, 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit-report-services	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-reportservices/credit-fraud-alerts
Experian	P.O. Box 2002 Allen, TX, 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/fraud/center.html

TransUnion	P.O. Box 1000 Chester, PA, 19016-1000 1-800-888-4213 www.transunion.com m	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze	P.O. Box 2000 Chester, PA, 19016-2000 1-800-680-7289 www.transunion.com/fraud-alerts
-------------------	--	---	--

For more information about fraud alerts, security freezes, and steps for avoiding identity theft, or if you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you can contact the Federal Trade Commission (FTC) at: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington D.C. 20580, by phone at 1-877-438-4338, or by visiting www.consumer.ftc.gov. You should also report incidents of suspected identity theft to local law enforcement and the Attorney General's office in your home state and file a police report.

- District of Columbia residents may contact the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, <https://oag.dc.gov>, or by phone at (202) 442-9828 (consumer protection hotline).
- Iowa and Oregon residents are advised to report any suspected identity theft to law enforcement, to their respective Attorney General, and to the FTC.
- If you are a Maryland resident, you may contact the Maryland Office of the Attorney General, Consumer Protection Division Office, at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023, or 410-528-8662, or at <https://www.marylandattorneygeneral.gov/Pages/contactus.aspx>.
- North Carolina residents may contact the North Carolina Office of the Attorney General, Consumer Protection Division, at 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, or by phone at 1-877-566-7226.
- Rhode Island residents may contact the Office of the Attorney General at 150 South Main Street, Providence, RI 02930, or by phone at (401) 274-4400.
- Massachusetts residents are advised of their right to obtain a police report in connection with this incident.
- New York residents, in addition to considering placing a security freeze on their credit reports, may report any incidents of suspected identity theft to law enforcement, including the FTC, the New York Attorney General, or local law enforcement. More information is available at the New York Department of State Division of Consumer Protection website, <https://dos.nysits.acsitefactory.com/consumerprotection>; The NY Attorney General at: <https://ag.ny.gov> or by phone at 1-800-771-7755; or via the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or <https://www.identitytheft.gov/#/>.