



October 21, 2022

**By Email (Idtheft@oag.state.md.us)**  
Office of the Attorney General, Maryland

**Orrick, Herrington & Sutcliffe LLP**

701 5<sup>th</sup> Avenue, Suite 5600  
Seattle, WA 98104

+1 206-839-4300

[orrick.com](http://orrick.com)

**Joseph Santiesteban**

E [jsantiesteban@orrick.com](mailto:jsantiesteban@orrick.com)

D +1 206-839-4300

F +1 206-839-4301

RE: Notice of Data Security Incident / See Tickets US

To Whom It May Concern:

We are writing on behalf of our client, Vivendi Ticketing US LLC (d/b/a See Tickets US) (“See Tickets” or the “Company”), to notify you of a data security incident. See Tickets identified activity indicating potential unauthorized access by a third party to certain event checkout pages on the See Tickets website in April 2021. See Tickets promptly launched an investigation with the assistance of a forensics firm and took steps to shut down the unauthorized activity. See Tickets’ response efforts had multiple phases and resulted in the complete shutdown of the unauthorized activity on January 8, 2022.

In the following months, See Tickets worked with Visa, MasterCard, American Express, and Discover to identify potentially affected pages and transactions. This wide-ranging effort was supported by multiple forensics firms, and included coordination with law enforcement. On September 12, 2022, See Tickets identified the individuals whose information may have been affected. While See Tickets’ investigation continues and See Tickets is not certain exactly which payment cards were affected, the Company is notifying individuals now out of an abundance of caution based on available information.

Affected information may include the data individuals provided when purchasing event tickets on certain See Tickets or Ticketon event pages between June 25, 2019, and January 8, 2022, including: name, address, zip code, payment card number, card expiration date, and CVV number. See Tickets does not store individuals’ Social Security numbers, state identification numbers, or bank account information.

See Tickets is committed to safeguarding its customers’ personal information. The Company has taken steps to deploy additional safeguards onto its systems, including by further strengthening its security monitoring, authentication, and coding.

Maryland Attorney General

October 21, 2022

Page 2

See Tickets began notifying individuals about this event via email on October 21, 2022. Based on available information, the payment card information of approximately 1,698 Maryland residents was potentially affected in the incident. This number represents an outer bound, however, as the Company's investigation into potentially narrower dates of unauthorized activity on various event checkout pages continues. A sample copy of the individual notice is attached.

If your office requires any further information in this matter, please contact me at (206) 839-4300 or [jsantiesteban@orrick.com](mailto:jsantiesteban@orrick.com).

Sincerely,

/s/ Joseph Santiesteban

Joseph Santiesteban

Partner

Orrick, Herrington, & Sutcliffe, LLP

Re: Notice of Data Breach

Dear {{User.UserAttributes.FirstName}} {{User.UserAttributes.LastName}},

See Tickets US writes to inform you about a data security incident that may have affected certain of your payment card information. Please review this notice. It provides important information about the incident, our response, and available resources.

### **What Happened?**

{{User.UserAttributes.VariableSentence}} See Tickets was alerted to activity indicating potential unauthorized access by a third party to certain event checkout pages on the See Tickets website in April 2021. We promptly launched an investigation with the assistance of a forensics firm and took steps to shut down the unauthorized activity. Our response efforts had multiple phases and resulted in the complete shutdown of the unauthorized activity in early January 2022. In the following months, we worked with Visa, MasterCard, American Express, and Discover to identify potentially affected pages and transactions. This wide-ranging effort was supported by multiple forensics firms, and included coordination with law enforcement. On September 12, 2022, we determined the event may have resulted in unauthorized access to the payment card information of certain of our customers. While our investigation continues and we are not certain your information was affected, we are notifying you out of an abundance of caution based on available information.

### **What Information Was Involved?**

Affected information may include the data you provided when purchasing event tickets on the See Tickets website between June 25, 2019, and January 8, 2022, including: name, address, zip code, payment card number, card expiration date, and CVV number.

*We do not store your Social Security number, state identification number, or bank account information.*

### **What We Are Doing**

See Tickets is committed to safeguarding our customers' personal information, and we value your privacy. We have taken steps to deploy additional safeguards onto our systems, including by further strengthening our security monitoring, authentication, and coding.

### **What You Can Do**

It is always a good idea to check your recent bank and/or credit card statement for any charges not authorized by you. If you see anything suspicious, you should immediately notify your financial institution. Even if you do not see any suspicious charges, you may want to call them to discuss possible options for avoiding potential problems in the future. Additional information about how to protect your identity is contained below.

It is always a good practice to remain vigilant against threats of identity theft or fraud, and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity. If you ever suspect that you are the victim of identity theft or fraud, you can contact your local police. Additional information about how to protect your identity is below.

It is also always a good idea to be alert for "phishing" emails by someone who acts like they know you or are a company that you may do business with and requests sensitive information over email, such as passwords, government identification numbers, or bank account information.

### **For more information:**

If you have questions regarding this notice, please reach out to us through our normal support channels or by calling 1-855-532-1424, 8:00am-5:30pm Central Time, Monday through Friday, excluding major U.S. holidays.

Sincerely,

James Murphy

**Chief Operations Officer**

**Vivendi Ticketing US LLC (Db a See Tickets US)**

## Information for U.S. Customers

### **MORE INFORMATION ABOUT IDENTITY PROTECTION**

#### **INFORMATION ON OBTAINING A FREE CREDIT REPORT**

U.S. customers 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 reports, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free (877) 322 8228.

#### **INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE**

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

##### **Equifax**

Consumer Fraud Division  
P.O. Box 740256  
Atlanta, GA 30374  
(888) 766 0008  
[www.equifax.com](http://www.equifax.com)

##### **Experian**

Credit Fraud Center  
P.O. Box 9554  
Allen, TX 75013  
(888) 397 3742  
[www.experian.com](http://www.experian.com)

##### **TransUnion**

TransUnion LLC  
P.O. Box 2000  
Chester, PA 19022 2000  
(800) 680 7289  
[www.transunion.com](http://www.transunion.com)

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382 4357; or [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

## ADDITIONAL RESOURCES

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, or the FTC.

**California Residents:** Visit the California Department of Justice's Privacy Unit (<https://oag.ca.gov/privacy>) for additional information on protection against identity theft.

**District of Columbia Residents:** The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; [oag@dc.gov](mailto:oag@dc.gov), and [www.oag.dc.gov](http://www.oag.dc.gov).

**Iowa Residents:** The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, +1 (515) 281-5164, [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov). You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**Maryland Residents:** The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov).

**Massachusetts Residents:** Under Massachusetts law, you have the right to obtain any police report filed in connection to the cybersecurity event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**North Carolina Residents:** The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (919) 716-6400; or [www.ncdoj.gov](http://www.ncdoj.gov).

**New Mexico Residents:** You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit [www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf](http://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf) or [www.ftc.gov](http://www.ftc.gov).

**New York Residents:** The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341, +1 (800)-771-7755; or [www.ag.ny.gov](http://www.ag.ny.gov).

**Rhode Island Residents:** The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; +1 (401) 274-4400; or [www.riag.ri.gov](http://www.riag.ri.gov). You may also file a police report by contacting local or state law enforcement agencies.



**DLA Piper LLP (US)**  
One Liberty Place  
1650 Market Street  
Philadelphia, PA 19103-7300  
[www.dlapiper.com](http://www.dlapiper.com)

Ron Plesco  
[Ron.plesco@us.dlapiper.com](mailto:Ron.plesco@us.dlapiper.com)  
T 215.656.2453

**VIA EMAIL:** [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us)

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

**September 5, 2023**

**RE: Notice of Data Event**

Dear Sir or Madam:

We represent Vivendi Ticketing US LLC d/b/a See Tickets (“See Tickets”) and are writing to notify your Office of a compromise that may affect the security of certain personal information relating to 1,478 Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, See Tickets does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of Maryland data event notification statute, or personal jurisdiction.

**Notice of Data Event**

In May 2023, See Tickets became aware of unusual activity on certain of its e-commerce websites. In response, See Tickets began working with third-party cyber forensic specialists to determine the nature and extent of the compromise, secure its websites, and identify what information may have been affected and to whom it relates.

In May and June of 2023, See Tickets’ third-party cyber forensic specialists determined that an unauthorized party(ies) inserted multiple instances of malicious code into a number of its e-commerce checkout pages resulting in unauthorized access to, and acquisition of, certain customer payment card information used to make purchases on the websites between February 28, 2023 and July 2, 2023. Once the forensic specialists determined the dates of compromise, See Tickets took steps to identify potentially impacted customers who made purchases during this time period. This process completed on July 21, 2023, See Tickets moved quickly to notify impacted individuals.

Please also note that as part of its response to this compromise, See Tickets took steps to implement additional safeguards to further protect the security of payment card information on its websites. Additionally, See Tickets notified law enforcement.

The information impacted includes the cardholder's name, address, and payment card information.

### **Notice to Maryland Residents**

On September 5, 2023, See Tickets began providing written notice of the compromise to potentially affected individuals, which includes 1,478 Maryland residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

### **Other Steps Taken and to be Taken**

Upon discovery of the compromise, See Tickets moved quickly to investigate and respond to the compromise, assess the security of its systems, and notify potentially affected individuals. See Tickets also reviewed its existing policies and procedures and implemented additional safeguards to further secure its systems and the information contained therein.

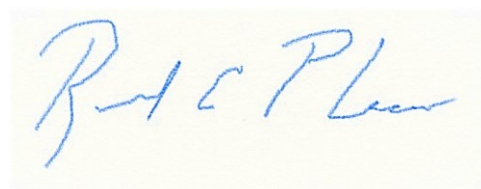
Additionally, See Tickets is providing individuals with guidance on how to protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their cred card company and/or bank. conducted a diligent investigation to confirm the nature and scope of the compromise. See Tickets is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national credit reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports, and encouragement to contact the Federal Trade Commission, their Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Although there is no evidence to suggest the personal information involved in this compromise has been fraudulently used, See Tickets is nevertheless providing individuals with access to twelve months of complementary credit monitoring and identity restoration services through Kroll.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the compromise, please contact me at (215) 656-2453.

Sincerely,



Ron Plesco