October 21, 2022

Orrick, Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, WA 98104

+1 206-839-4300
orrick.com

Joseph Santiesteban

E jsantiesteban@orrick.com
D +1 206-839-4300
F +1 206-839-4301

By U.S. Certified Mail
Consumer Protection Bureau,
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

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.

See Tickets began notifying individuals about this event via email on October 21, 2022. Based on available information, the payment card information of approximately 12,976 New Hampshire 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.

Sincerely,

Joseph Santiesteban
Partner
Orrick, Herrington, & Sutcliffe, LLP

See TICKETS

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 (Dba 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 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	**Experian**	**TransUnion**
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022 2000
(888) 766 0008	(888) 397 3742	(800) 680 7289
www.equifax.com	www.experian.com	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.

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, and 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. 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.

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.

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 or 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.

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. You may also file a police report by contacting local or state law enforcement agencies.