

[ADDRESS]

Dear [NAME],

Notice of Data Breach

ShowTix4U recently became aware of a potential security incident possibly affecting the personal information of certain individuals who made a payment card purchase on the ShowTix4U.com website. We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened

We were recently alerted by our payment card processor to a potential security incident involving our website. Based upon an ongoing forensic investigation, it appears that an unauthorized actor was able to gain access to our third-party vendor's server and install malicious software on our website. The malicious software appears designed to capture payment card information as the information was inputted.

What Information Was Involved

We believe that the incident could have affected certain information (including name, address, email address, telephone number, payment card account number, expiration date, and card verification code) of individuals who made a purchase on the website between December 11, 2016, and February 2, 2017. According to our records, you made a payment card transaction on the website during that timeframe and your information may be affected. Please note that because we do not collect sensitive personal information like Social Security numbers, this type of sensitive information was not affected by this incident.

What We Are Doing

We take the privacy of personal information seriously, and deeply regret that this incident occurred. We've taken steps to address this incident promptly after we were alerted to it, including engaging outside forensic experts to assist us in investigating, remediating the situation, and transitioning away from the third-party vendor that hosted our website. The incident has been contained. In addition, the incident has been reported to federal law enforcement and we are cooperating with their investigation.

What You Can Do

As always, we encourage you to regularly review your credit card statements and report any suspicious or unrecognized activity immediately to your financial institution. We are working with the card brands who will notify your financial institutions or yourself, if necessary, of steps that will or can be taken to secure your credit card information. In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

Please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert at no cost or a security freeze on your credit file.

For More Information

If you have additional questions or concerns about this incident, you may contact us at 866-981-6854 between 9am-5pm Pacific or email support@showtix4u.com. Again, we sincerely regret any concern this event may cause you.

Sincerely,

ShowTix4U

Information about Identity Theft Protection

Review Accounts and Credit Reports: You can also 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 by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number 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 get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)

General Contact:

P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:

P.O. Box 740256, Atlanta, GA 30374

Credit Freezes:

P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)

General Contact:

P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:

P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)

General Contact:

P.O. Box 105281
Atlanta, GA 30348
877-322-8228

Fraud Alerts and Security Freezes:

P.O. Box 2000, Chester, PA 19022
888-909-8872