NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2758
kris.kleiner@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

October 28, 2015

By Certified Mail
Return Receipt Requested

Hawaii Office of Consumer Protection
Leiopapa A Kamehameha Building
235 South Beretania Street, Suite 801
Honolulu, Hawaii 96813

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Digital Theatre, LLC ("Digital Theatre"), operator of the ShowTix4U website (the "Website"), to inform you of a security incident involving personal information provided to Digital Theatre, LLC that may have affected approximately 1,453 Hawaii residents. Digital Theatre, LLC is notifying these individuals and outlining some steps they may take to help protect themselves.

On October 9, 2015, after an extensive forensic investigation, Digital Theatre learned that unauthorized individuals installed malicious software on the computer server hosting the Website. The company believes the malware could have compromised the personal information of customers that made credit or debit card purchases through the Website between April 19 and September 30, including name, address, payment card account number, card expiration date, and payment card security code.

Digital Theatre takes the privacy of personal information seriously, and deeply regrets that this incident occurred. The company engaged a computer forensic investigator to perform an investigation and help address this incident. Following the discovery of the incident, Digital Theatre secured any possible intrusion points and took appropriate steps to further strengthen our network defenses. In addition, the company has outsourced payment screens to a third party and has undergone security vulnerability scanning, code review, and is certified as PCI compliant.

Affected individuals are being notified via written letter, with these notifications scheduled to be sent between October 30, 2015 and November 4, 2015. Form copies of the notices being sent to affected Hawaii residents are included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2758 or kris.kleiner@nortonrosefulbright.com.

Very truly yours,

Kristopher Kleiner

KCK
Enclosure

Dear [NAME],

Digital Theatre, LLC, operator of the ShowTix4U website (the "Website"), recently became aware of a security incident possibly affecting the personal information of certain individuals who made a payment card purchase on the Website. We are providing this notice as a precaution to inform potentially affected customers of the incident and to call your attention to some steps you can take to help protect yourself. We sincerely apologize for any frustration or concern this may cause you.

What Happened

Although our independent forensic investigation is ongoing, at this time, we believe that between late April 2015 and late September 2015 unauthorized individuals installed malicious software on a computer server hosting the Website. According to our records, you made a payment card purchase on the Website during that timeframe and your information may be at risk. While Digital Theatre does not store credit card information, we believe the malware could have compromised the personal information (name, address, payment card account number, card expiration date, and payment card security code) of customers that made credit card purchases through the Website.

We take the privacy of personal information seriously, and deeply regret that this incident occurred. We took steps to address and contain this incident immediately after it was discovered, including engaging outside forensic experts to assist us in investigating and remediating the situation. Following the discovery of the incident, we secured any possible intrusion points, took appropriate steps to further strengthen our network defenses, and payment screens have been outsourced to a third party. The website is PCI compliant. We are also conducting a data forensics investigation of this incident with assistance from a leading computer security firm so those responsible for illegal access of the server can be prosecuted. While our investigation and security improvements are ongoing, we are confident that our customers can safely use payment cards on the Website.

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 of steps that will or can be taken to secure your credit card information.

We recommend that you continue to check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. Also, 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 or a security freeze on your credit file.

We are very sorry that this happened and for any uncertainty or inconvenience this has caused you. Please be assured while we are continually strengthening and evolving our defenses based on new and emerging threats, the website is PCI compliant, no credit card information is stored, and customers can safely use payment cards on the website. For additional questions please contact 866-981-6854. We appreciate your business and take the security of your information very seriously.

Sincerely,
Digital Theatre

Information about Identity Theft Protection

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 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 us and 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

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

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

Equifax (www.equifax.com)
P.O. Box 105851
Atlanta, GA 30348
800-685-1111

Fraud Alerts:
P.O. Box 105069, Atlanta, GA 30348
Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
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)
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