

STATE OF NH
DEPT OF JUSTICE

2015 MAR -6 AM 11:23

 NORTON ROSE FULBRIGHT

March 3, 2015

**By Certified Mail
Return Receipt Requested**



Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Kraft Music LTD ("Kraft," operator of the kraftmusic.com website: the "Website") to inform you of a security incident involving personal information provided to Kraft that affected approximately 5 New Hampshire residents. Kraft is notifying these individuals and outlining some steps they may take to help protect themselves.

On February 3, 2015, Kraft 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 December 21, 2014 and February 3, 2015, including name, address, payment card account number, card expiration date, and payment card security code.

Kraft takes the privacy of personal information seriously, and deeply regrets that this incident occurred. Kraft took steps to address this incident once it was discovered, including the following: the company (i) initiated an internal investigation in collaboration with its web server host and was able to promptly contain the incident, (ii) removed the malicious software, (iii) installed new security patches, and (iv) installed software that checks the Website code on an hourly basis for modifications. Kraft has also hired a PCI Qualified Security Assessor to help identify and implement additional security measures that may be appropriate.

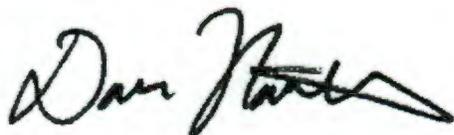
Affected individuals are being notified via written letter, which includes an offer for one year of complimentary identity protection and fraud resolution services. These notifications will begin mailing on or around March 3, 2015. Form copies of the notices being sent to affected New Hampshire residents are included for your reference.

Office of the New Hampshire Attorney General
March 3, 2015
Page 2

NORTON ROSE FULBRIGHT

If you have any questions or need further information regarding this incident, please contact me

Very truly yours,



Partner
Co-Chair, Data Protection, Privacy & Access
to Information

DJN/smm
Enclosure



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<FirstName>><<LastName>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name>>,

Kraft Music LTD ("Kraft") is writing to inform you of an incident involving personal information you provided while using www.kraftmusic.com (the "Website"). For more than thirty years, Kraft has worked to earn your trust and business, and we value our relationship with you. As a precaution, we are providing this notice and outlining some steps you may take to help protect yourself. We sincerely apologize for any frustration or concern this may cause you.

On February 3, 2015, we learned that unauthorized individuals installed malicious software on the computer server hosting the Website and took certain personal data entered by our customers. It appears that the initial compromise occurred on December 21, 2014 and ended on February 3, 2015. The malicious software and fraudulent use of our website could have compromised the information of customers that made purchases on our Website, including name, address, payment card account number, card expiration date, and payment card security code. According to our records, you made a payment card purchase at the Website during that timeframe and your information may be at risk.

Kraft takes the privacy of personal information seriously, and deeply regrets that this incident occurred. We took steps to address this incident promptly after it was discovered. We initiated an internal investigation in collaboration with our web server host and were able to contain the incident within hours of its discovery. We removed the malicious software, installed new security patches and installed software that checks our website code on an hourly basis for modifications. We have also hired a PCI Qualified Security Assessor to help identify and implement additional security measures that may be appropriate.

We want to make you aware of steps you can take to guard against fraud or identity theft. We recommend that you review your credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor your statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

We also recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. Also, please review the enclosed "Information about Identity Theft Protection" reference guide that describes additional steps you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection, and details on how to place a fraud alert or a security freeze on your credit file.

In addition, to help protect your identity, we have partnered with CSID to provide one year of complimentary CSID Protector services. CSID is a provider of identity protection and fraud detection solutions and technologies and will provide you with increased visibility into possible fraudulent activity so that you can respond more quickly if such activity is detected. You will also have a team of Identity Restoration Specialists to guide you through the recovery process should you become the victim of identity theft. We encourage you to activate your CSID Protector coverage as quickly as possible, but no later than June 6, 2015, by visiting <http://www.csid.com/csidprotector-en7> and entering the following PIN Code <<PIN CODE>>. (Note this PIN code can only be used once and is non-transferable.) Please refer to the reverse side of this letter for further information and instructions on completing the enrollment process.

Finally, you may contact us directly if you have any questions or concerns regarding this incident by calling 1-800-783-3368 (choose option 3) between the hours of 10:00 AM and 6:00 PM (Central Time), Monday through Friday (excluding holidays). Again, we are sorry for any inconvenience or concern this event may cause you.

Sincerely,

Ben Kraft, President

CSID Protector Services

The sign-up process for your one-year complimentary CSID Protector services is conducted online via CSID's secure website, <http://www.csid.com/csidprotector-en7>. Should you have any questions regarding the coverage or the sign-up process, please contact CSID Member Services at 1-855-568-2999 24/7 or email support@csid.com. Once you have enrolled and created your username and password, you will return to CSID's page to log in and access your personal information on future visits.

CSID Protector includes:

- **CyberAgent®:** CSID's exclusive Internet surveillance technology scours websites, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information online
- **Identity Restoration:** Work with a certified identity theft restoration specialist, who will work on your behalf to restore your identity and let you get on with your life

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 below.

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 above.

National Credit Reporting Agencies:

Equifax
P.O. Box 105788
Atlanta, GA 30348
877-478-7625
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
800-680-7289
www.transunion.com