James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

May 15, 2017

INTENDED FOR ADDRESSEE(S) ONLY
VIA EMAIL & U.S. 1ST CLASS MAIL

Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
Email: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent KURU Footwear, 4416 S Century Dr, Salt Lake City, UT 84123 ("KURU"), and are writing to notify your office of an incident affecting KURU's e-commerce site, www.kurufootwear.com, that may affect the security of personal information relating to certain Washington residents. By providing this notice, KURU does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 2, 2017, KURU began investigating some unusual activity reported by its credit card processor. KURU immediately began to work with third-party forensic experts to investigate these reports and to identify any signs of compromise on its systems. On February 23, 2017, KURU discovered that it was the victim of a sophisticated cyber-attack that resulted in the potential compromise of some customers' debit and credit card data used at www.kurufootwear.com between December 20, 2016 to March 3, 2017.

Since that time, KURU has been working with third-party forensic investigators to determine what happened, what information was affected and to implement additional procedures to further protect the security of customer debit and credit cards. KURU removed the malware at issue to prevent any further unauthorized access to customer debit or credit card information. KURU is also working with the Federal Bureau of Investigations to investigate this incident. Customers can safely use their payment card at www.kurufootwear.com.

Notice to Washington Residents

Through the ongoing third-party forensic investigations, KURU confirmed on February 23, 2017 that malware may have stolen credit or debit card data from some credit and debit cards used at www.kurufootwear.com between December 20, 2016 and March 3, 2017. The information at risk as a result of this event includes the cardholder's name, address, card number, expiration date and CVV. KURU determined that personally identifiable information relating to five hundred and thirteen (513) Washington residents may have been compromised. KURU is providing written notice of this incident to these potentially impacted Washington residents beginning on or about May 15, 2017, in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

KURU is working with the FBI to investigate this incident. KURU has established a dedicated hotline for individuals to contact with questions or concerns regarding this incident. Additionally, KURU is providing potentially impacted individuals with helpful information on how to protect against identity theft and fraud, including how to place a fraud alert and security freeze on one's credit file, the contact information for the national consumer reporting agencies, 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 free credit reports, and encouragement to contact the Federal Trade Commission, state attorney general, and law enforcement to report attempted or actual identity theft and fraud. KURU is also providing written notice of this incident to other state regulators and the national consumer reporting agencies as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4798.

Very truly yours,

James E. Prendergast of
MULLEN COUGHLIN LLC

JEP:ncl

Enclosure

EXHIBIT A

KURU

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

We recently learned that we were the victims of a sophisticated cyber-attack that may affect the security of your payment information. We are providing you with information about the incident, steps we are taking in response, and steps you can take to protect against fraud should you feel it is appropriate.

What Happened? On February 2, 2017, we began investigating some unusual activity reported by our credit card processor. We immediately began to work with third-party forensic experts to investigate these reports and to identify any signs of compromise on our systems. On February 23, 2017, we discovered that we were the victim of a sophisticated cyber-attack that resulted in the potential compromise of some customers' debit and credit card data used at www.kurufootwear.com between December 20, 2016 and March 3, 2017.

Since that time, we have been working with third-party forensic investigators to determine what happened, what information was affected and to implement additional procedures to further protect the security of customer debit and credit cards. We removed the malware at issue to prevent any further unauthorized access to customer debit or credit card information. We are also working with the Federal Bureau of Investigations to investigate this incident. Through this process, we can now confirm you can safely use your payment card at our website.

What Information Was Involved? Through the ongoing third-party forensic investigations, we confirmed on February 23, 2017 that malware may have stolen credit or debit card data from some credit and debit cards used at www.kurufootwear.com between December 20, 2016 and March 3, 2017. The information at risk as a result of this event includes the cardholder's name, address, card number, expiration date and CVV.

What We Are Doing. We take the security of our customers' information extremely seriously, and we apologize for the inconvenience this incident has caused. We continue to work with third-party forensic investigators and law enforcement officials to ensure the security of our systems.

What You Can Do. Please review the enclosed Privacy Safeguards Information for additional information on how to better protect against identity theft and fraud. We encourage you to remain vigilant against incidents of identity theft by reviewing your account statements regularly and monitoring your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of their credit report.

For More Information. We are very sorry for any inconvenience or concern this incident causes you. The security of your information is a priority for us. Should you have any questions about the content of this letter or ways you can better protect yourself from the possibility of identity theft, we encourage you to call the dedicated assistance line, staffed by professionals who are experienced in working through situations like this, at 888-738-0532 between 9:00 a.m. and 9:00 p.m. EST, Monday through Friday, excluding major holidays.

Sincerely,

Bret Rasmussen
Chief Executive Officer
KURU Footwear

PRIVACY SAFEGUARDS INFORMATION

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents please call 1-800-349-9960)
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
PO Box 2000
Chester, PA 19022-2000
1-888-909-8872
www.transunion.com/securityfreeze

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 50 Rhode Island resident may be impacted by this incident. Customers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, customers will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed as a result of a law enforcement investigation.