

May 1, 2017

Bruce A. Radke  
Shareholder  
+1 312 609 7689  
[bradke@vedderprice.com](mailto:bradke@vedderprice.com)**VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)  
AND FEDERAL EXPRESS**The Honorable Joseph Foster  
Attorney General of the State of New Hampshire  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301**Re: Notification of a Computer Security Incident**

Dear Attorney General Foster:

We represent Nathan Sports ("Nathan"). Nathan is reporting a potential unauthorized disclosure of unencrypted computerized data containing the personal information of three (3) New Hampshire residents pursuant to N.H. REV. STAT. ANN. § 359-C:20.

The investigation of this incident is ongoing, and this notice will be supplemented, if necessary, with any significant new facts discovered subsequent to its submission. By providing this notice, Nathan does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction in connection with this incident.

**Background of the Incident**

Nathan ([www.nathansports.com](http://www.nathansports.com)), headquartered in Fountain Valley, CA, is the market leader in creating ground-breaking Running Essentials™ gear. Nathan running products are available in specialty running shops, outdoor retailers, and sporting goods stores in 45 countries and online.

On April 11, 2017, Nathan discovered the personal information of three (3) New Hampshire residents may have been affected when an external actor or actors placed hidden code on the Nathan web servers (the "Incident"). The code may have targeted certain personal information of customers who made credit card purchases via the Nathan web servers, including those customers' first and last names, billing or mailing addresses, e-mail addresses and credit card information (card holder names, credit card account numbers, expiration months and years and card security codes).

Upon learning of the incident, Nathan promptly launched an internal investigation and retained a leading incident response and digital forensics firm to assist in Nathan's investigation. Nathan promptly notified its customers as soon as possible after the investigation was completed and Nathan determined the identities of the potentially affected customers.

**Notice to New Hampshire Residents**

On April 28, 2017, Nathan will be notifying the three (3) New Hampshire residents of the incident. Attached is a sample of the notification letter that is being sent to the affected New Hampshire residents via first-class United States mail.

In addition, Nathan has established a confidential telephone inquiry line to assist the affected customers with any questions they may have regarding this incident. This confidential inquiry line is available between 9:00 a.m. and 5:00 p.m., ET, Monday through Friday, at 855 474-3871.

**Other Steps Undertaken and to Be Undertaken by Nathan**

Nathan has already begun taking several actions to help prevent this type of incident from occurring in the future. These actions include evaluating ways to best strengthen its systems to guard against this type of similar future incident and working with its network vendors to implement additional security controls on its website.

**Contact Information**

Please contact me if you have any questions or if I can provide you with any further information concerning this matter. Thank you.

Yours very truly,

Bruce A. Radke

BAR/bah  
cc: Dennis Goetz, Chief Financial Officer



NATHAN

c/o GCG  
PO Box 10455  
Dublin, OH 43017-4055

SMP1000002



Sample Customer  
123 Sample St  
Apt 2  
Dublin, OH 43017



STATE OF NH  
DEPT OF JUSTICE

2017 MAY -3 AM 10: 09

c/o GCG  
PO Box 10455  
Dublin, OH 43017-4055

SMP1000002



April 28, 2017

Sample Customer  
123 Sample St  
Apt 2  
Dublin, OH 43017

Dear Sample Customer,

Nathan Sports (“Nathan”) values and respects your privacy, which is why we are writing to advise you about a recent incident that may affect your personal information, steps that Nathan has undertaken since discovering the incident, and information on what you can do to better protect yourself, should you feel it is appropriate to do so.

On April 6, 2017, Nathan discovered that your personal information may have been affected when an external actor or actors placed hidden code on the Nathan webservers (the “Incident”). The code may have targeted certain personal information of customers who made credit card purchases via the Nathan webservers between September 5, 2016 and November 11, 2016, including those customers’ first and last names, billing or mailing addresses, e-mail addresses and credit card information (card holder names, credit card account numbers, expiration months and years and card security codes).

Upon learning of the incident, Nathan promptly launched an internal investigation and commenced containment and remediation efforts. Nathan also retained a leading incident response and digital forensics firm to assist in Nathan’s investigation. In addition to conducting an extensive internal investigation, Nathan has already begun taking several actions to help prevent this type of incident from occurring in the future. These actions include evaluating ways to best strengthen our systems to guard against this type of similar future incident and working with our network vendors to implement additional security controls.

We value the trust you place in Nathan to protect the privacy and security of your personal information, and we apologize for any inconvenience or concern that this incident might cause you. We have established a confidential telephone inquiry line to assist you with any questions you may have regarding this incident. This confidential inquiry line is available, at no cost to you, between 9:00 a.m. and 5:00 p.m., Eastern time, Monday through Friday, at 855 474-3871.

Sincerely,

Dennis Goetz  
Chief Financial Officer, United Sports Brands



## Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

**Credit Reports:** You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting <http://www.annualcreditreport.com>, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at: <https://www.annualcreditreport.com/cra/requestformfinal.pdf>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax  
1-800-349-9960  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 105788  
Atlanta, GA 30348

Experian  
1-888-397-3742  
[www.experian.com](http://www.experian.com)  
P.O. Box 9554  
Allen, TX 75013

TransUnion  
1-888-909-8872  
[www.transunion.com](http://www.transunion.com)  
P.O. Box 2000  
Chester, PA 19022

**Fraud Alerts:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at <http://www.annualcreditreport.com>.

**Credit and Security 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 on your credit file, 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 cause a delay should you attempt to obtain credit. In addition, you may incur fees for placing, lifting and/or removing 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:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013

TransUnion Security Freeze  
Fraud Victim Assistance Department  
P.O. Box 6790  
Fullerton, CA 92834

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.

This notice has not been postponed at the request of a law enforcement agency.

**Iowa Residents:** You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General  
1305 E. Walnut Street

Des Moines, IA 50319  
(515) 281-5164  
[www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov)

**Maryland Residents:** Maryland residents can contact the Office of the Attorney General at regarding steps they can take to avoid identity theft:

Office of the Attorney General  
220 St. Paul Place  
Baltimore, MD 21202  
(888) 743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

**North Carolina Residents:** North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

North Carolina Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
(877) 566-7226  
[www.ncdoj.com](http://www.ncdoj.com)