LANE POWELL

DARIN M. SANDS
503.778.2117
sandsd@lanepowell.com

JULIE M. ENGBLOOM
503.778.2183
engbloomj@lanepowell.com

August 16, 2017

CONFIDENTIAL

VIA ELECTRONIC MAIL
attorneygeneral@doj.nh.gov

Mr. Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Data Incident Notification
Our File No.: 130795.0002

Dear Attorney General MacDonald:

We are writing on behalf of our client, Native Canada Footwear Ltd. ("Native Shoes"), which has learned of an electronic security vulnerability and possible breach of personal information that may have affected some consumers in your state.

On June 23, 2017, Native Shoes became aware of a potential vulnerability in the security of its website. Native Shoes immediately took the system offline that day and hired well-respected forensics firms to conduct a full investigation into what had happened. Through that investigation, Native Shoes learned that malware had infected the Native Shoes website as early as April 2015. It appears to have resided in the website until the system was taken offline on June 23, 2017. This malware may have allowed outside parties to acquire payment-related information from customers who made Visa and Mastercard purchases through the Native Shoes website. Native Shoes is notifying all consumers who may have been affected.

The data potentially affected for those customers is:

- Credit or debit card information used to make purchases on the Native Shoes website
- The names, addresses, email addresses, and telephone numbers of customers

Notifications are being sent to consumers in your state, based on customers who made purchases from the website between April 28, 2015, and June 23, 2017, in the form of the letter attached hereto. In New Hampshire, approximately 70 customers were affected and will receive this notice. Native Shoes has also launched a dedicated website, at nativeshoes.com/08-08-17/breach-help, and a dedicated telephone hotline, at (866) 685-6159, to answer customers' questions about this incident. As set out in the letter, Native Shoes is also offering consumers a year of credit monitoring at the expense of Native Shoes.

In addition to the investigation of this incident, Native Shoes is conducting a thorough review of its electronic systems, including those not involved in this incident. Native Shoes has retained respected forensic and cyber security professionals to test its electronic systems and to upgrade security efforts across Native Shoes's electronic systems. Further, Native Shoes took the systems affected by this incident offline during investigation, and they will remain offline. Last, Native Shoes is developing a new online shopping site, which will run on an entirely redesigned and upgraded platform.

If you have any questions about this incident, Native Shoes's response, or Native Shoes's notifications to consumers, please contact Darin Sands and Julie Engbloom at Lane Powell PC, at the contact information listed above.

Very truly yours,

LANE POWELL PC

Darin M. Sands
Julie M. Engbloom

DMS
Attachment

130795.0002/7044540.1

Notice of Data Breach

August 16, 2017

<<Address1>>
<<Address2>>
<<City>> <<State>> <<Zip10>>
<<CountryName>>

Dear: <<NAME1>>

Native Shoes recently learned that our computer systems were the victim of a criminal malware attack. Upon learning of a potential vulnerability, we immediately took our systems offline and engaged well-respected forensics firms to conduct a full investigation into what had happened. We have also informed relevant law enforcement and regulatory authorities of this investigation.

What Happened?

Native Shoes became aware of a potential vulnerability in the security of our website in late June 2017 and immediately launched an investigation. That investigation has confirmed that malware may have infected the Native Shoes website as early as April 2015. As a result, we are informing you that it is possible that your payment information was compromised if you bought shoes from nativeshoes.com using Visa or Mastercard between April 28, 2015, and June 23, 2017. If that payment information was indeed stolen, your information may be affected.

What Information Was Involved?

Based on the facts known to the company at this time, the personal information at-issue may have included:

- Credit or debit card information used to buy from nativeshoes.com
- Your name, address, email address, and telephone number

This incident does not affect purchases outside of nativeshoes.com. If you bought through one of our online partners, or at a brick-and-mortar store, that payment information is not at risk from this incident. Also, purchases made on our website using PayPal are not affected.

What We Are Doing

The security and privacy of your information is a top priority for us. Native Shoes has retained respected forensic and cyber security professionals to assist us in investigating this incident. Upon discovery of the malware, Native Shoes immediately took the affected system permanently offline. Native Shoes has also developed a new online shopping website, which will run on an entirely redesigned, upgraded platform.

What You Can Do

As a courtesy, Native Shoes has arranged for CyberScout to provide daily credit monitoring of your TransUnion credit file, a credit report and access to cyber monitoring at no cost to you for one year, at your option. The steps to sign up for these services are included in the attached Reference Guide, which also provides additional information about steps you can take to monitor and protect against unauthorized use of your personal information.

Out of an abundance of caution, we recommend that you contact your credit card company to request that they re-issue your credit cards with new account numbers. Additionally, we encourage you to be diligent in watching for unauthorized charges on your payment cards and to quickly report any suspicious activity to your bank or credit card company. The phone number to call is usually on the back of the credit or debit card.

You can also contact the three major credit reporting agencies to discuss your options. You have the right to place a credit freeze on your credit file, which will require potential creditors to contact you before opening new accounts. To place a fraud alert on your credit report contact the three U.S. credit reporting agencies below.

Experian	Equifax	TransUnion
(888) 397-3742	(877) 478-7625	(800) 916-8800
P.O. Box 9532	P.O. Box 740241	P.O. Box 2000
Allen, TX 75013	Atlanta, GA 30374-0241	Chester, PA 19016
www.experian.com	www.equifax.com	www.transunion.com

You can obtain a free copy of your credit report from each of the three nationwide consumer reporting agencies by calling 1-877-322-8228 or online at: www.annualcreditreport.com. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three major credit reporting agencies. You may want to obtain copies of your credit report to ensure the accuracy of the report information.

To learn more about protecting yourself from identity theft and to report incidents of identity theft, you can visit the Federal Trade Commission's websites at www.consumer.gov/idtheft, www.ftc.gov/credit, or by calling call 1-877-5-NO-SCAM (1-877-566-7226). You may also receive information from the Federal Trade Commission's office by writing to:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

For More Information

If you have any other questions regarding this incident or need more information, we have set up a toll-free, hotline number, **(866) 685-6159**, where operators are available between 9:00AM and 5:00PM EASTERN TIME, MONDAY THROUGH FRIDAY, to answer your questions. You can also visit our website at nativeshoes.com/08-08-17/breach-help, where we have posted additional information.

While incidents of this kind have unfortunately become more common, we want you to know that we are working hard to minimize any inconvenience this incident may cause you. Native Shoes is also committed to investing significant time and energy in review and testing of our electronic security, and enhancements to our security policies, procedures and practices.

We greatly appreciate your loyalty to the Native Shoes brand, and deeply apologize for any inconvenience or concern this might have caused.

Very truly yours,

Kyle R. Housman

Kyle Housman
President, Native Canada Footwear, Ltd.

Directions for Enrolling in CyberScout's credit and identity theft protection product, FraudScout*, offered by Native Shoes

FraudScout provides daily credit file monitoring of your TransUnion credit report which alerts you within 24 hours of a key change reported on your file. This product also provides access to your TransUnion credit report and cyber monitoring which monitors thousands of websites, chat rooms, forums and networks, and alerts you to if your personal information is being bought or sold online. Items monitored can include your credit or debit card numbers, email address, phone number and other information.

To enroll, please visit https://www.myidmanager.com and follow the instructions provided. When prompted please provide the following unique code to receive services: <<CODE>>

Reference Guide - U.S. State Notification Requirements

For residents of *California, Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, New Mexico, North Carolina, Oregon, Rhode Island, Vermont, Virginia, Washington, West Virginia* and *Wyoming*:

Pursuant to state law, we advise you to remain vigilant for incidents of fraud and identity theft by regularly reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a free credit report, whether or not you suspect any unauthorized activity on your account, online by visiting www.annualcreditreport.com, or by calling toll-free at 1-877-322-8228. You may also obtain a free credit report 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

You may also obtain a copy of your credit report by contacting any one or more of the national consumer reporting agencies listed below. They can also provide you with additional information about fraud alerts and security freezes.

Experian	Equifax	TransUnion
(888) 397-3742	(877) 478-7625	(800) 916-8800
P.O. Box 9532	P.O. Box 740241	P.O. Box 2000
Allen, TX 75013	Atlanta, GA 30374-0241	Chester, PA 19016
www.experian.com	www.equifax.com	www.transunion.com

For residents of *Illinois, Massachusetts, Rhode Island* and *West Virginia*:

Information Regarding Fraud Alerts

A fraud alert is a notice placed on your credit file that alerts creditors that you could be a victim of fraud. Fraud alerts are designed to encourage creditors to take additional steps to verify your identity before creating new credit accounts in your name or taking other actions related to your credit, such as increasing credit limits or adding a card to a pre-existing credit or debit card account.

There are three types of fraud alerts that last for varying time-periods: (1) initial fraud alerts, which last for 90 days, (2) extended fraud alerts, which last for 7 years and (3) for military personnel, active duty alerts, which last for 1 year. To place a fraud alert on your account, contact one of the three major credit reporting agencies

Experian	Equifax	TransUnion
(888) 397-3742	(877) 478-7625	(800) 916-8800
P.O. Box 9532	P.O. Box 740241	P.O. Box 2000
Allen, TX 75013	Atlanta, GA 30374-0241	Chester, PA 19016
www.experian.com	www.equifax.com	www.transunion.com

Placement of a Security Freeze on your Credit File

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit file, you need to send a request to a consumer reporting agency by certified mail, overnight mail or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit freeze for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The cost of placing, removing, or temporarily lifting a security freeze varies by state, but generally costs between $5 and $20 for each action at each credit reporting company.

Under Massachusetts law, we are required to inform you that if you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift or permanently remove a security freeze.

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For residents of *Iowa* and *Oregon*:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for certain law enforcement entities is as follows:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
http://www.doj.state.or.us
1-(877)-877-9392

Iowa Attorney General
Div. of Consumer Protection
1305 E. Walnut Street
Des Moines, IA 50319
www.iowaattorneygeneral.gov
(515) 281-5926

For residents of *California, Illinois, Maryland, North Carolina* and *Rhode Island*:

State laws require us to tell you that you can obtain information from the Federal Trade Commission about steps you can take to avoid identity theft (including how to place a fraud alert or security freeze). Your state also may offer guidance about how you can prevent or respond to identity theft. In particular, you may report instances of identity theft to your state's Attorney General or to your local police or sheriff's department. Relevant contact information appears below.

MD Attorney General's Office
Consumer Protection Division
200 St. Paul Place 9001
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

NC Attorney General's Office
Consumer Protection Division
Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
http://www.ncdoj.gov

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400

California Attorney General's Office
California Department of Justice
Attn: Office of Privacy Protection
P.O. Box 944255
Sacramento, CA 94244-2550
Telephone: (916) 322-3360
Toll-free in California: (800) 952-5225

For residents of *Massachusetts* and *Rhode Island*: You have a right to obtain a police report relating to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of *Florida* and *West Virginia*: You may call us at 1 (866) 685-6159 to learn what types of information, if any, we maintain about you and other individuals.

For residents of *California* and *Wyoming*: this letter has not been delayed by a law enforcement investigation.