VedderPrice

Chicago
New York
Washington, DC
London
San Francisco
Los Angeles
Singapore
vedderprice.com

Bruce A. Radke
Shareholder
+1 312 609 7689
bradke@vedderprice.com

November 30, 2017

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 This Works Products, Ltd. ("This Works"). This Works is reporting a potential unauthorized access of unencrypted computerized data containing the personal information of one (1) New Hampshire resident 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, This Works 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

This Works (thisworks.com) is an award-winning British skincare brand, known for its targeted skin solutions, formulated with a super-blend of proven actives, botanical oils and therapeutic fragrance and created to work in harmony with a person's body clock. Founded in 2003 the company is now available in over 20 countries worldwide, including the United Kingdom, United States of America, Canada and Australia.

On October 19, 2017, This Works discovered that the personal information of one (1) New Hampshire resident may have been affected when a third party gained unauthorized access to This Works' online ordering system (the "Incident"). The external actor may have acquired certain personal information of customers who made credit card purchases via the This Works online ordering system (www.thisworks.com), including those customers' names, email addresses, home addresses, shipping addresses, phone numbers and credit card information (credit card account numbers, expiration months and years, and Card Verification Value ("CVV") code).

Upon learning of the Incident, This Works promptly launched an internal investigation and immediately took steps to secure its website and prevent any further intrusion. This Works also retained a leading

incident response and digital forensics firm to assist in This Works' investigation. While we have identified the potential window of compromise, due to the nature of the Incident, it has not been possible to confirm conclusively whether or not any customers' information was taken or used. Nevertheless, in an abundance of caution, This Works promptly notified all of its potentially affected customers as soon as possible after the investigation was completed.

Notice to the New Hampshire Resident

On November 30, 2017, This Works will be notifying the one (1) New Hampshire resident of the Incident. Attached is a sample of the notification letter that is being sent to the affected New Hampshire resident via first-class United States mail. In addition, This Works has established a confidential telephone inquiry line to assist the affected customers with any questions they may have regarding this Incident.

Other Steps Undertaken and to Be Undertaken by This Works

The IT forensics specialist has provided confirmation that This Works' website is now secured from the unauthorized third party's further access. This Works has also taken additional steps to strengthen security and will continue to do so in the future.

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: Joe Fletcher, eCommerce Director, This Works Products, Ltd.

thisworks®
24HR SKIN SOLUTIONS

November 30, 2017

<<Name>>
<<Address>>
<<City>>, <<State>><<Zip Code>>

Dear <<Name>>,

As a valued This Works customer, we wanted to write to you to let you know about a recent data security incident that may have affected some of your personal information that you gave to us while shopping.

On October 19, 2017, we became aware of suspicious activity on our website network leading us to believe an unlawful intrusion had occurred. We immediately took steps to secure our website and prevent any further intrusion. Since then, we have worked with an external IT forensics specialist to help us carry out a thorough investigation in order to understand what happened and which of our customers might have been affected.

We believe that a third party gained unauthorized access to the online ordering system of www.thisworks.com from September 5, 2017 to October 19, 2017. Due to the nature of the attack it has not been possible to confirm conclusively whether or not your personal information was taken or used. It is possible, however, that the third party accessed some of the details you submitted in our order form. This includes your name, e-mail address, home address, shipping address, phone number and payment card details (including credit card account number, expiration month and year and Card Verification Value ("CVV") code) used for the transaction.

The IT forensics specialist has provided confirmation that our website is now secured from this third party's further access. We have taken additional steps to strengthen security and will continue to do so in the future. However, we wanted to notify all our customers that could have been affected so that you can take preventative measures to safeguard against any third-party use of your data, including those listed in the Additional Important Information on the following page.

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 6:00 p.m., Central Time, Monday through Friday, at 888-451-6558.

This Works values your privacy and deeply regrets that this incident occurred.

Joe Fletcher
eCommerce Director
This Works Products, Ltd.

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 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
P.O. Box 105788
Atlanta, GA 30348

Experian
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
1-888-909-8872
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.

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

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

Office of the Attorney General
220 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
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