

November 30, 2017

DIRECT DIAL 216.696.5787 | paul.janowicz@tuckerellis.com

Attorney General Gordon J. MacDonald
New Hampshire Department of Justice
Attn: Data Security Breach
33 Capitol Street
Concord, NH 03301

RECEIVED

DEC 01 2017

CONSUMER PROTECTION

Re: *Suspected Data Security Breach Notification
IdeaStream Consumer Products, LLC*

Dear Mr. MacDonald:

We are writing in connection with N.H. Rev. STAT. § 359-C:20 on behalf of our firm's client, IdeaStream Consumer Products, LLC ("IdeaStream Consumer Products"). It is our understanding that on November 1, 2017, IdeaStream Consumer Products learned it may have been the victim of a cyber-attack. Specifically, VividFront, LLC ("VividFront"), which designed and manages IdeaStream Consumer Products' website, informed IdeaStream Consumer Products that it had discovered that an unauthorized party had compromised a portion of IdeaStream Consumer Products' website's code after running a security scan. The malicious code was immediately quarantined and deleted. On November 3, 2017, however, IdeaStream Consumer Products was informed that malicious code had been reinstalled. As a result, IdeaStream Consumer Products took its website offline until it could conduct a more thorough investigation.

Based on our investigation, it is our understanding that the malicious code recorded customer information in an online file while online transactions were being processed and may have affected customers who made purchases on IdeaStream Consumer Products' website from August 29, 2017 to November 3, 2017. The potentially compromised information includes customer names, e-mail addresses, mailing addresses, and payment information, including credit card information. No social security numbers were compromised.

Since learning of the compromised code, IdeaStream Consumer Products has been working with VividFront to gather information, ensure the malicious code has been removed, and strengthen the security on IdeaStream Consumer Products' website. IdeaStream Consumer Products has also retained an independent forensic expert to assist with the investigation and provide additional security recommendations. IdeaStream Consumer Products is in the process of implementing those recommendations.

In light of the potential disclosure of customer information, a copy of the attached notice will be mailed to all potentially affected New Hampshire residents on or about December 1, 2017. Based on our investigation, we believe that one (1) New Hampshire resident who provided IdeaStream Consumer Products with information was potentially affected.

As you will see, IdeaStream Consumer Products is offering a year of credit monitoring services to all potentially affected individuals, has opened a call center to answer any questions those individuals may have, and has advised consumers on additional steps they may take to protect themselves from potential identity theft.

If you have any questions, please do not hesitate to contact us.

Sincerely,

TUCKER ELLIS LLP

A handwritten signature in blue ink, appearing to be "R. Hanna" and "P. Janowicz" combined.

Robert J. Hanna
Paul L. Janowicz



RETURN MAIL PROCESSING CENTER
PO BOX 6336
PORTLAND, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>> <<Date>>

Dear <<Name1>>:

NOTICE OF DATA BREACH

What Happened?

We are writing to notify you that information you previously provided to IdeaStream Consumer Products while shopping on our website may have been acquired by a third-party without permission. On November 1, 2017, the company that manages our website informed us that they had detected malicious code on our site while running a security scan. The malicious code was immediately quarantined and deleted. On November 3, 2017, however, IdeaStream Consumer Products learned that malicious code had been reinstalled. As a result, IdeaStream Consumer Products took its website offline until it could conduct a more thorough investigation.

Based on our investigation, it appears the malicious code captured customer information while transactions were being processed and recorded the information in an online file. It is our current understanding that the malicious code may have recorded the information of customers who made purchases on IdeaStream Consumer Products' website from approximately August 29, 2017 to November 3, 2017.

What Information Was Involved?

The information potentially disclosed includes customer names, e-mail addresses, mailing addresses, and payment information, including credit card information. No social security numbers were disclosed.

What Are We Doing?

Since learning of the malicious code and taking our website offline, IdeaStream Consumer Products has been working with our outside website manager to gather facts, prevent any further disclosures of customer information, and strengthen our website's security. We have also retained an independent information technology firm to assist with the investigation and provide additional security recommendations for IdeaStream Consumer Products' website. IdeaStream Consumer Products is in the process of implementing their recommendations. Notice of this incident was not delayed as a result of any law enforcement investigation.

What Can You Do?

We want to make you aware of important steps you can take to protect yourself against identify theft and fraud.

First, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

812 Huron Rd East, Ste. 390
Cleveland, OH 44115
216-459-2400

To enroll in this service, go to the *myTrueIdentity* website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code <<Enrollment Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<Engagement Number>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Second, we recommend that you regularly review your credit and debit card account statements to determine if there has been any unauthorized activity. If you notice any unusual activity, you should contact the bank that issued the debit or credit card immediately.

In addition, you are entitled to obtain a free copy of your credit report once a year. A credit report contains important information about your credit history and the status of your credit accounts. You can obtain a copy of your credit report by contacting one of the following national consumer reporting agencies:

Equifax
PO Box 740256
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19016
800-680-7289
www.transunion.com

In order to further protect yourself, you may also want to consider placing either a fraud alert or security freeze on your credit file. A **FRAUD ALERT** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires the business to verify your identity before issuing you credit. Although this may cause a short delay if you are the one applying for credit, it can help protect against someone else obtaining credit in your name. A **SECURITY FREEZE** prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Please be aware, however, 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. You can obtain additional information about fraud alerts and security freezes, including any fees you may be required to pay in order to place a fraud alert or security freeze on your credit file, by contacting the credit reporting agencies listed above or the Federal Trade Commission, whose contact information is listed below. There may be a fee for placing, temporarily lifting, or removing a Security Freeze with each of the nationwide consumer reporting companies, although that fee is waived if you send the credit reporting company proof of eligibility by mailing a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

If you notice any suspicious activity with your accounts or suspect you are the victim of identity theft, you have the right to and should report the incident to your local law enforcement office, your state Attorney General, and/or the Federal Trade Commission. The contact information for the Federal Trade Commission is:

Federal Trade Commission
Bureau of Consumer Protection
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

812 Huron Rd East, Ste. 390
Cleveland, OH 44115
216-459-2400

For Maryland Residents

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place, 16th Floor
Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov

For North Carolina Residents

You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office at:

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

For Rhode Island Residents

You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
1-401-274-4400
www.riag.ri.gov

For More Information

If you have any questions regarding the incident, please call 1-877-494-9829.

We sincerely apologize for any inconvenience you may experience as a result of this incident. We thank you in advance for your continued support and confidence in IdeaStream Consumer Products.

Sincerely,

Daniel Parella
President and Chief Operating Officer
IdeaStream Consumer Products, LLC

812 Huron Rd East, Ste. 390
Cleveland, OH 44115
216-459-2400