LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

April 8, 2019

VIA E-MAIL
Attorney General Gordon J. MacDonald
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
E-mail: *DOJ-CPB@doj.nh.gov*

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent America Juice Co., LLC ("America Juice") with respect to a recent data security incident described in greater detail below. America Juice takes the protection of sensitive customer information very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. **Nature of the security incident.**

In November 2018, America Juice learned of suspicious activity on its website server. Upon discovering this activity, America Juice took immediate steps to secure its system and began an internal investigation. America Juice also engaged an independent computer forensics firm to conduct an investigation into the suspicious activity and to determine whether, and to what extent, any personally identifiable information ("PII") of its customers may have been affected. The results of that investigation indicate that the names, addresses, credit card information, and customer profile information for customers of America Juice may have been involved.

2. **Number of New Hampshire residents affected.**

America Juice notified seventeen (17) residents of New Hampshire residents regarding this data security incident. Notification letters were mailed via first class U.S. mail on April 8, 2019. A sample copy of the notification letter sent to potentially impacted individuals is included with this letter.

3. Steps taken relating to the incident.

America Juice has taken steps in response to this incident to further strengthen the security of its e-commerce web platform in an effort to prevent similar incidents from occurring in the future. America Juice also reported the matter to the payment card brands to protect its customers' payment card information and prevent fraudulent activity. In addition, America Juice is providing twelve months of complimentary Cyber Monitoring services through CyberScout, a company that specializes in identity theft education and resolution.

4. Contact information.

America Juice remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (214) 722-7141 or by e-mail at Lindsay.Nickle@lewisbrisbois.com.

Respectfully,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

LBN:arb

Encl.: Consumer Notification Letter

Name
Address
Address2
City, state zip

<<Date>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notification of Data Security Incident

Dear <<First Name>> <<Last Name>>:

I am writing on behalf of America Juice Co., LLC ("AJC") and X2O Vapes to inform you of a data security incident that may have affected your personal information. At AJC, we take the privacy and security of your information very seriously and regret any concern that this incident may cause you. That is why we are contacting you and informing you about steps you can take to protect your information.

What happened? In November 2018, we learned of suspicious activity on our website server. Upon discovering the activity, we took immediate steps to further secure our system and conducted a thorough internal investigation to determine the scope of the problem. We also engaged an independent computer forensics firm to conduct an investigation into what happened and to help us determine whether customer information was accessed or acquired without authorization.

What information was involved? After an extensive forensics investigation and diligent review of the customer information that may have been affected, we determined that the incident may have involved your name, address, credit card information, and customer profile information.

What we are doing. As soon as we discovered the incident, we took the steps discussed above. In addition, we reported the matter to the payment card brands to protect your payment card information and prevent fraudulent activity. In order to prevent similar incidents from occurring in the future, we are actively implementing additional measures to further enhance the security of our e-commerce web platform. In addition, we are providing you with twelve months of Cyber Monitoring* services at no cost to you. The Cyber Monitoring will review the dark web and alert you if your personal information is found online. These services will be provided by CyberScout, a company that specializes in identity theft education and resolution.

To enroll in Cyber Monitoring* services at no charge, please log on to https://www.myidmanager.com and follow the instructions provided. **When prompted, please provide the following unique code to receive services: <<CODE>>.**

What you can do. You can follow the recommendations on the following page to protect your personal information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have occurred, you should contact the bank that issued the credit or debit card immediately.

For more information: We remain committed to protecting your information. For guidance with the CyberScout services, or to obtain additional information, please call our dedicated help line at **1-800-405-6108**, 8:00 a.m. to 5:00 p.m. Central, Monday through Friday, and supply the fraud specialist with your unique code.

Thank you for your loyalty and your patience through this incident. We take your trust in us and this matter very seriously. Please accept our apologies for any worry or inconvenience this may cause you.

Sincerely,

Joe Deighan
CEO | America Juice Co., LLC

Services marked with an "" require an internet connection and e-mail account. 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.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review 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 incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 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 also contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Free Annual Report
P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
www.annualcreditreport.com

Fraud Alert: 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 the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
Marylandattorneygeneral.gov
1-888-743-0023

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.