NuCO2
BEVERAGE CARBONATION MADE EASY

October 14, 2011

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Delaney,

I am writing to you on behalf of $NuCO_2$ Inc. ("$NuCO_2$") to notify your office of a recent incident that involves the personal information of certain $NuCO_2$ employees, approximately three of whom are residents of your state. On September 26, 2011, $NuCO_2$ became aware that a company laptop computer belonging to one of our employees was stolen. The stolen computer contained the names and U.S. Social Security Numbers of certain residents. We do not believe that the computer contained any resident's date of birth, financial account information, or other sensitive personally identifying information. We have no evidence that the personal information of any resident has been misused.

The theft was reported to local law enforcement authorities in Atlanta, Georgia. Upon learning of the theft, we took immediate steps to investigate the information that may have been contained on the stolen computer and the extent of any possible compromise of personal information. We are also enhancing our information security policies and procedures to prevent future incidents.

On October 17, 2011 we began sending the enclosed notification letter by mail to all individuals whose information was contained on the stolen computer. In addition, we have engaged Kroll Inc. to provide services to affected individuals, at no charge to them, to help safeguard their identity. These services include one year of credit monitoring.

Sincerely,

Peter M. Green
Senior Vice President and General Counsel
$NuCO_2$ Inc.

Enclosure: Resident Notification Letter

NuCO2
BEVERAGE CARBONATION MADE EASY

ID TheftSmart™

<<FirstName>> <<MiddleName>> <<LastName>>
Membership Number: <<MembershipNumber>>

Member Services: 1-800-XXX-XXXX
9:00 a.m. to 6:00 p.m. (Eastern Time), Monday through Friday
If you have questions or feel you may have an identity theft issue, please call ID TheftSmart member services.

URGENT — Please Open Immediately.

<<FirstName>> <<MiddleName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<StateProvince>> <<PostalCode>>
<INTELLIGENT MAIL BARCODE>

<<Date>> (Format: Month Day, Year)

Dear <<FirstName>> <<MiddleName>> <<LastName>>,

We recently learned that a company laptop computer belonging to a $NuCO_2$ employee was stolen. Unfortunately, there was a file on that computer that contained your name and U.S. Social Security number. At this time, we have no evidence that your personal information has been misused. However, to protect against possible identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, to monitor your credit reports and to consider the additional steps described in the *Reference Guide* enclosed with this letter.

In addition, because securing your personal information is very important to us, we have engaged Kroll Inc., the world's leading risk consulting company, to provide you, at no charge, with its ID TheftSmart™ service for one year. Kroll's Fraud Solutions team has more experience than any other organization when it comes to helping people who have experienced the unintentional exposure of confidential data. Kroll's ID TheftSmart service provides:

Enhanced Identity Theft Consultation and Restoration. Licensed Investigators who truly understand the problems surrounding identity theft are available to listen, to answer your questions, and to offer their expertise regarding any concerns you may have. And should your name and credit be affected by this incident, your investigator will help restore your identity to pre-theft status.

Current Credit Report. Kroll offers you access to an up-to-date credit report from Experian.

Continuous Credit Monitoring. Monitoring alerts make you aware of key changes, using data from all three major national credit repositories, in your credit file that could indicate the kind of unauthorized activity commonly associated with identity theft and fraud.

If you would like to take advantage of Kroll's ID TheftSmart service—again, at no charge to you—please see the enclosed brochure for easy enrollment instructions. To receive online credit services, please visit www.idintegrity.com to complete your authorization. To receive offline credit services through the mail, please complete and return the enclosed *Consumer Credit Report and Credit Monitoring Authorization Form*. Note, however, that you cannot enroll online if you use the *Consumer Credit Report and Credit Monitoring Authorization Form*.

If you have any questions or feel you may have an identity theft issue, you may call Kroll at 1-XXX-XXX-XXXX, 9:00am – 6:00pm (Eastern time), Monday through Friday.

We deeply regret that this happened, and we are enhancing our information security policies and procedures to prevent future incidents. We trust that the quality and reliability of the support services being offered demonstrate our continued commitment to your security and well being.

Sincerely,

Vicki Strauss
Senior Vice President, Operations
$NuCO_2$ Inc.

Reference Guide

To protect against possible identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, to monitor your credit reports and to consider these additional steps:

Security Freeze. Some state laws allow you to place a security freeze on your credit reports. This would prohibit a credit reporting agency from releasing any information from your credit report without your written permission. You should 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. The specific costs and procedures for placing a security freeze vary by state law, but this reference guide provides general information. You can find additional information at the websites of any of the three credit reporting agencies listed below.

If you believe that you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it will not charge you to place, lift or remove a security freeze on your credit reports. In all other cases, a credit reporting agency may charge you up to $5.00 (and in some cases, up to $20.00) each time you place, temporarily lift, or permanently remove a security freeze.

Requirements vary by state, but generally to place a security freeze on your credit report, you must send a written request to each of the three credit reporting agencies noted below, which must include the following information: (1) full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security Number; (3) date of birth; (4) addresses for the prior five years; (5) proof of current address; (6) a legible copy of a government issued identification card; (7) a copy of any relevant police report, investigative report, or complaint to a law enforcement agency concerning identity theft and (8) if you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash though the mail.

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348
877-478-7625
www.equifax.com

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

TransUnion Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, California 92834-6790
800-680-7289
www.transunion.com

Free Credit Reports. To order a free copy of your credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three national credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security Number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

Fraud Alerts. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert advises you of an attempt by an unauthorized person to open a new credit account in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a free fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus. You can also place a fraud alert on your credit report online at the websites listed below for Equifax and Experian and via email for TransUnion at fvad@transunion.com.

Equifax
P.O. Box 105069
Atlanta, Georgia 30348-5069
800-525-6285
www.fraudalerts.equifax.com

Experian
P.O. Box 1017
Allen, Texas 75013
888-397-3742
www.experian.com

TransUnion Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, California 92834-6790
800-680-7289
www.transunion.com

Police Report. If you find suspicious activity on your credit reports or account statements, or have reason to believe that your personal information is being misused, contact your local law enforcement authorities immediately and file a police report. You have the right to request a copy of the police report and should retain it for further use, as many creditors want the information it contains to absolve you of potential fraudulent debts.

Consulting the FTC. In addition to your state Attorney General, you can contact the FTC to learn more about how to protect yourself from identity theft:

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

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (toll-free in North Carolina)
919-716-6400
www.ncdoj.gov

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
888-743-0023 (toll-free in Maryland)
410-576-6300
www.oag.state.md.us