INFORMATIONLAWGROUP
privacy. security. technology. media. intellectual property.

March 6, 2013

VIA CERTIFIED MAIL RETURN RECEIPT REQUESTED

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams,

I write on behalf of Frontier Natural Products Co-op ("Frontier"), operator of www.auracacia.com, www.simplyorganic.com, www.frontiercoop.com and www.wholesale.frontiercoop.com ("Websites"), to inform you of a security incident involving personal information of approximately 101 residents of your State. Frontier is notifying these individuals and outlining some steps they may take to help protect themselves.

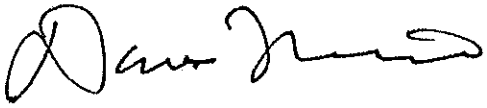
On or about January 31, 2013, Frontier discovered that a malicious person had added a file to a computer server that hosts the Websites. As a result of the modification, from September 14, 2012 to January 31, 2013, the malicious person was able to gain access to the server and intercept certain personal information as it was inputted by users making purchases at the Websites, and obtain access to a customer database residing on the server. Frontier believes that that the personal information of some of its customers could have been taken as a result of this incident, including name, address, city, state, telephone, username, password and payment card information, such as card number, expiration date and security codes (e.g. CVV2/CVC2/CID).

Frontier takes the privacy of personal information seriously. Frontier took immediate action to address and contain the incident the same day it was discovered by removing a malicious file involved in the incident and repairing an application that may have been compromised. Frontier also conducted an extensive investigation of this event, which included the use of internal investigators and a third party forensic investigator to carefully review the impacted systems and data so Frontier could accurately understand the scope of the incident and determine other remediation steps. As a result, Frontier has implemented more safeguards including additional layers of intrusion detection security. Finally, Frontier notified law enforcement of this incident and intends to assist their efforts in prosecuting the criminals who accessed our systems.

Frontier is notifying affected individuals via written letter and has arranged for affected US residents to be eligible to enroll for and receive twelve months of free identity monitoring services provided by First Watch Technologies, Inc. These notifications will begin mailing on or around March 6, 2013. A copy of the form of notices being sent to impacted residents of your State is attached for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 325-3528 or dnavetta@infolawgroup.com

Sincerely,



David Navetta, Esq., CIPP/US
Partner, InfoLawGroup LLP

Enclosure

Return mail will be processed by: IBC
P.O. Box 802
Fort Mill, SC 29716
PO #121822A

1 1 00000001 238487

FRONTIER®
NATURAL PRODUCTS CO-OP

3021 78th Street, PO Box 299
Norway, IA 52318

,

March 6, 2013

Dear :

We are writing to inform you of a security incident involving personal information maintained by Frontier Natural Products Co-op ("Frontier"), operator of www.auracacia.com, www.simplyorganic.com, www.frontiercoop.com and www.wholesale.frontiercoop.com ("Websites"). While we do not know if your personal information has been (or will be) misused, out of an abundance of caution, we are providing this notice and outlining some steps you may take to help protect yourself. We sincerely apologize for any inconvenience or concern this may cause you.

Summary of Incident

On or about January 31, 2013, Frontier discovered that a malicious person had added a file to a computer server that hosts the Websites. As a result of the modification, from September 14, 2012 to January 31, 2013, the malicious person was able to gain access to the server and intercept certain personal information as it was inputted by users making purchases at the Websites, and obtain access to a customer database residing on the server. We believe that your personal information could have been taken as a result of this incident, including name, address, city, state, telephone, username, password and payment card information, such as card number, expiration date and security codes (e.g. CVV2/CVC2/CID). Please be aware that a small number of the Websites' users have told us that their payment cards were used for fraudulent transactions after visiting the Websites during that timeframe.

Frontier's Response

We value our relationship with you and sincerely regret that this incident took place. Keeping your personal information secure is of the utmost importance to us, and we are taking steps to help prevent this type of incident from happening in the future. Frontier took immediate action to address and contain the incident the same day it was discovered by removing a malicious file involved in the incident and repairing an application that may have been compromised. Frontier also conducted an extensive investigation of this event, which included the use of internal investigators and a third party forensic investigator to carefully review the impacted systems and data so Frontier could accurately understand the scope of the incident and determine other remediation steps. As a result, Frontier has implemented more safeguards including additional layers of intrusion detection security. Finally, Frontier notified law enforcement of this incident and intends to assist their efforts in prosecuting the criminals who accessed our systems.

Recommended Steps

We want to make you aware of steps you can take to guard against identity theft or fraud. At this time, we recommend that you review your credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. You should continue to monitor your statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, call the bank that issued your credit or debit card immediately.

We also recommend you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office. Also, please review the enclosed "Information about Identity Theft Protection" reference guide that describes additional steps you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection, and details on how to place a fraud alert or a security freeze on your credit file.

In addition, to help safeguard you from misuse of your personal information, we have arranged for you to receive identity monitoring services provided by First Watch Technologies, Inc. for twelve months at no cost to you. You can sign up for this service anytime between now and May 31, 2013 using the verification code listed below. To enroll in this service, simply call 877-817-0173 between the hours of 9:00 AM and 7:00 PM (Eastern Time) Monday through Friday (excluding holidays), or go to http://www.firstwatchid.com and:

- Click on verification code on the upper right-hand corner of the First Watch ID homepage.
- Enter the appropriate information including your unique 12-digit verification code: **1234 5678 9012**.

Please be aware that you will not receive these services unless you complete the enrollment.

After enrolling, First Watch ID will monitor thousands of databases and billions of records in the United States on your behalf to look for suspicious activity that could indicate the beginning steps of identity theft. If suspicious activity is found, First Watch will place a personal phone call to you (at the telephone number that you provide) to determine if the suspicious activity is potentially fraudulent.

Additionally, First Watch provides you with easy access (at http://www.firstwatchid.com) to the credit bureaus' service that allows you to monitor your credit by requesting one free credit report annually from each of the three major credit bureaus. First Watch suggests that you request your free report from one bureau at a time every four months. First Watch provides you with an email reminder service (if you sign-up) that notifies you every four months to request your report from the appropriate credit bureau. The First Watch ID service also includes up to $25,000 of identity theft insurance with $0 deductible, along with identity restoration coverage (certain limitations and exclusions may apply*).

Finally, we have established a call center to answer questions from individuals affected by this incident. You may call 866-263-4159 between the hours of 9:00 AM and 7:00 PM (Eastern Time), Monday through Friday (excluding holidays), to address additional questions or concerns you may have. Again, we are sorry for any inconvenience or concern this event may cause you.

Sincerely,

Tony Bedard
Chief Executive Officer
Frontier Natural Products Co-op

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or 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, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790
800-685-1111	888-397-3742	800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against 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 residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below:

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 9532	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 6790
877-478-7625	888-397-3742	Fullerton, CA 92834-6790
www.equifax.com	www.experian.com	800-680-7289
		www.transunion.com

Credit 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, 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 delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove 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
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

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.