BRYAN CAVE

BRYAN CAVE LP

bryancave.com

RECEIVED

SEP 12 2017

CONSUMER PROTECTION

September 11, 2017

Joshua A. James
Direct: 202/508-6265
Fax: 202/220-7565
josh.james@bryancave.com

CONFIDENTIAL

VIA FEDEX

State of New Hampshire Department of Justice Office
of the Attorney General Joseph Foster
33 Capitol Street
Concord, NH 03301

Re: Voluntary Data Security Breach Notification

To Whom It May Concern:

Frontier Natural Products Co-Op ("Frontier"), a client of Bryan Cave LLP, will be notifying 14 customers who reside in New Hampshire of a criminal cyber-attack on the Frontier e-commerce sites. This letter is being provided as a courtesy as we do not believe notification is required under N.H. Rev. Stat. 359-C:19.

In August, Frontier confirmed that customer information may have been impacted during a data security incident affecting its e-commerce website between May 12, 2017 and August 22, 2017.

While the investigation is ongoing, at this time Frontier believes that malicious code was added to the Frontier websites which allowed unauthorized individuals to capture certain payment information during the checkout process. The information potentially affected included customer name, shipping and billing address, and credit card number. Frontier has removed the malicious code and taken steps to help prevent unauthorized website access in the future.

Frontier has notified its payment processor of this incident. In addition, Frontier is notifying potentially affected customers on September 12, 2017. An example of the customer message is attached.

Frontier is offering each affected customer Kroll identity protection services which include identity restoration assistance and identity theft insurance. While there is no reason to believe that this event will result in new account creation identity theft, in order to assure customers who may be concerned, or confused, about that possibility, Frontier is also offering each affected customer one year of credit monitoring. Information regarding these services, as well as additional information to assist customers, is included in the notification sent to the customer.

If you would like any additional information concerning the above event, please feel free to contact me at your convenience.

Sincerely,

/s/ Joshua James

Joshua James

Attachment

ATTACHMENT

FRONTIER®
CO-OP
MEMBER OWNED SINCE 1976

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Dear <<MemberFirstName>> <<MemberLastName>>,

Re: ***Notice of Data Breach***

Frontier Cooperative takes our responsibility to protect our customers' privacy very seriously. That is why we are writing to you. We have discovered that, like many other businesses, government agencies, and professional firms, we were impacted by a data security incident that may have affected your payment card information.

What Happened? In August we confirmed that a data security incident could have impacted some visitors to our websites who placed orders between Friday, May 12, 2017 and Tuesday, August 22, 2017. These sites include: Frontiercoop.com, Simplyorganic.com, Auracacia.com, or Coopmarket.com.

What Information Was Involved? While the investigation is still ongoing, we have confirmed the possibility that unauthorized individuals may have gained access to your name, the shipping and billing address, and the payment card number used to make your purchase on one of our sites.

This type of information typically does not result in new accounts being created using your identity. However, it may result in attempts to place fraudulent charges on your payment card so you should review your payment card accounts for suspicious activity.

What We Are Doing: The security of our customers' information is always a priority and we sincerely regret any inconvenience to you. We are contacting customers who may have been affected by this incident. As a precaution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **my.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.

*You have until **December 14, 2017** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-855-230-2963. Additional information describing your services is included with this letter.

What You Can Do: Please review the recommendations on the following page for steps you can take to protect your personal information and sign up for 12 months of complimentary identity protection services.

For More Information: If you have questions or concerns that are not addressed in this notice letter, please call 1-855-230-2963, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready.

We certainly apologize for any inconvenience this situation may cause and appreciate your past and future business.

Sincerely,

Nicole Erickson
Vice President of Finance
Frontier Co-Op

Important Information: Recommendations You Can Take to Protect Your Identity

TAKE ADVANTAGE OF YOUR IDENTITY PROTECTION SERVICES

You have been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

Review Your Accounts and Credit Reports

Regularly review statements from your payment card account to determine if there is any suspicious charge. Although the information involved in this incident is unlikely to lead to the creation of new accounts using your identity, as a general matter we recommend periodically obtaining your credit report from one or more of the national consumer reporting agencies. Pursuant to the Fair Credit Reporting Act (FCRA), you may obtain a free copy of your credit report online at www.annualcreditreport.com or by calling toll free 1.877.322.8228. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf. You may also contact one or more of the three national consumer reporting agencies listed below:

- Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241, 1.800.685.1111, www.equifax.com
- Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742, www.experian.com
- TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016, 1.800.916.8800, www.transunion.com

Be Aware of Possible Phishing

Phishing refers to someone who attempts to obtain your information by disguising themselves as someone that you may know or recognize. If you receive a suspicious email or telephone call that appears to be from us and that asks for personal information please call us directly to confirm whether it is, in fact, from us, and do not respond to it.

Place a Fraud Alert and Security Freeze

You may obtain information from the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. If you suspect you may be a victim of identity theft you may place a fraud alert in your file by calling one of the consumer reporting agencies listed above. The agency that you contact will notify the other two agencies. An initial fraud alert lasts 90 days. An extended alert stays on your file for seven years. To place either of these alerts a consumer reporting agency will require you to provide appropriate proof of your identity. If you ask for an extended alert, you will have to provide an identity theft report.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. The consumer reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. Unlike a fraud alert, you must separately place a credit freeze with each consumer reporting company. A consumer reporting agency may charge you a fee of up to $5 to place a security freeze, although there is typically no charge if you have been the victim of identity theft. Like a fraud alert, they may also require you to provide proof of your identity (such as your name, Social Security Number, date of birth, address, and/or a government issued ID card or a bill).

Additional Steps to Avoid Identity Theft

- ***Additional State Specific Resources.*** The following state agencies offer additional information and steps to avoid identity theft, and you may report suspected ID theft to them:

Maryland Attorney General
Identity Theft Unit
200 St. Paul Pl, 16th Floor
Baltimore, MD 21202
http://www.oag.state.md.us/idtheft/index.htm
888.743.0023

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx
919.716.6400

Oregon Attorney General
Department of Justice
1162 Court Street NE
Salem, OR 97301
https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/
503.378.4400

Iowa Attorney General
1305 E. Walnut St.
Des Moines, IA 50319
https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information/identity-theft/
515.281.5164

Rhode Island Attorney General
150 South Main St.
Providence, RI 02903
http://www.riag.ri.gov/ConsumerProtection/About.php
401.274.4400

Suggestions if You Are a Victim of Identity Theft

- ***File a police report.*** You can file a report with local law enforcement and ask to obtain a copy of the report to submit to any creditors that require proof of a crime.
- ***Contact the U.S. Federal Trade Commission (FTC).*** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.
- ***Keep a record of your contacts.*** Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.