1855 W. 2nd Ave
Eugene, Oregon 97402
(800) 953-5499

[date]

[Name]
[Address]
[City, State, Zip]

Subject: Data Security Incident

Dear [Name]:

I am writing to inform you of a data security incident that may have affected your personal information. We take the privacy and security of your information very seriously. This is why I am contacting you and informing you about steps that can be taken to protect your personal information.

What happened? On November 4th, 2016, we were informed that customer payment card information may have acquired without authorization. We immediately began an investigation, and confirmed that payment card information used to make online purchases on our site between September 26, 2016, and early November 5th, 2016, may have been acquired without our customer's authorization. We immediately scanned our system for malware, removed the malware, and the backdoor that allowed the code to be installed was identified and secured.

What information was involved? The following information may have been accessed: payment card information, including names, payment card numbers, security codes and expiration dates. It did not include debit or credit card PINs or bank account numbers. The credit card number we have record of use for your order is a [Card Type] Card ending with [Last 4 of credit card].

What are we doing? As soon as we were learned that customer payment card information may have been acquired without authorization, we immediately began an investigation, scanned for malware, removed the malware, and took measures to increase the security of our system. We also notified our merchant bank and the payment card networks so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used during the timeframe in which cards may have been compromised. Finally, the security of our system has been enhanced and the backdoor that allowed the code to be installed was identified and secured.

What you can do: You can follow the recommendations on the following page to protect your personal information. This may include reviewing your payment card account statements 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 also should 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 (FTC).

We encourage you to contact us should you have any questions. You can call us at 800-953-5499 ext. 5, email us at data@backcountrygear.com, We encourage you to change the password to the account you hold with us. We also recommend that you closely monitor your financial accounts and that you promptly contact your financial institution if you notice any unauthorized activity or contact your credit card company and request a new credit card be issued.

For more information: Further information about how to protect your personal information appears on the following page. We are grateful for your business and your trust. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Sincerely,

Michael Monson
Owner

(see reverse side)

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 by reviewing 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 also should 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 (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 print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	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: In some US states, 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. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. 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, Federal Trade Commission 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 Federal Trade Commission 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	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			