

12/5/18

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General:

We are writing to notify you of a breach of security and unauthorized access or use of personal information involving 6 New Hampshire residents.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

We were recently made aware of malicious software being attached to our website. Some payment information was potentially exposed. This information includes names, addresses, and payment account numbers as well as email addresses.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

There were 6 individuals that were affected in New Hampshire whose personal information was subject of this incident. We plan to mail a notice to the affected New Hampshire residents on December 11, 2018. We have included a copy of the notice to the affected New Hampshire residents.

STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

We take our responsibilities to protect our customer's information **very** seriously. The malicious software has been removed as of November 26, 2018 from our website and as a result of this incident, we have implemented security measures to ensure the confidentiality of the personal information of those we serve.

CONTACT INFORMATION

Please contact Timothy King, President of Backcountry Edge, Inc. at 717-665-1576 ext 101, tim@backcountryedge.com, if you have any questions or need further information.

Sincerely,

Timothy S. King
President

Name
Address
City, state zip

Backcountry Edge Inc.
708 Ditz Drive
Manheim, PA 17545



Toll Free: (800)617-0643
Fax: (717)665-0880

Date

Name

Address

Address

Address

Notice of a Data Breach

Dear:

Please read this letter in its entirety.

What happened?

We are writing to inform you of a recent security incident related to our website at www.backcountryedge.com. We were made aware of this situation on November 26, 2018, and our support provider took immediate steps to shut down unauthorized access to our website. Unfortunately, malicious code had already been executed resulting in the exposure of customer information.

What information was involved?

Based on the review of the situation and an examination of the impacted website, it is possible that some personal data belonging to you was potentially exposed to the unauthorized intruder. This data may have included some combination of your name, address, email address and payment card information.

While we have no evidence that any of your personal information was misused in any manner, we are taking appropriate precautionary measures to ensure your financial security and help alleviate concerns you may have.

What are we doing to address this situation?

Backcountry Edge has made immediate enhancements to our systems, security and practices. We are working with our support provider to implement additional tools designed to identify this type of threat and prevent it from happening. We are committed to helping those people who may have been impacted by this unfortunate situation. That's why Backcountry Edge is providing you with access to a fraud specialist to assist with any questions that you might have. These services will be provided by **CyberScout**, a company that specializes in identity theft education and resolution.

For guidance with the **CyberScout** services, or to obtain additional information about these services, **please call the CyberScout help line 1-800-405-6108** and supply the fraud specialist with your unique code. <cod>

What can you do to address this situation?

We are urging all customers to notify their issuing bank of this incident to inform them that your account may be at an increased risk for fraud and so that your bank can flag your account. We also encourage you to monitor your accounts

closely for any suspicious activity and to notify your financial institution immediately if you notice any unauthorized transactions.

Be sure to report any suspicious activity to Backcountry Edge or CyberScout.

Other Important Information

Please see the attached Additional Important Information for more information and other steps you can take.

For more information

While CyberScout should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with Backcountry Edge regarding this incident. If so, please call Customer Support at **800-617-0643** from 9:00 AM to 5:30 PM Eastern Time, Monday through Friday.

At Backcountry Edge we take our responsibilities to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

Timothy King
President and Founder

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax

P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian

P.O. Box 22104
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19022
1-800-888-4213
www.transunion.com

You may also 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.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Maryland, North Carolina, and Illinois:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

North Carolina Office of the Attorney General

Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission

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

For residents of Massachusetts:

State law requires you be informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below:

Experian (1-888-397-3742)

P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)

P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)

P.O. Box 2000
Chester, PA 19016
www.transunion.com

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/freeze/center.html>

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19016
<https://freeze.transunion.com>

You can also obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC):

Federal Trade Commission

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