20038

March 26, 2021

[redacted]

Dear [redacted],

We write to advise you that we were recently the victim of a data security incident (the "Incident"). We are writing to let you know how this Incident may have affected your personal information ("Information") and, as a precaution, to provide steps you can take to help protect your Information. We are contacting you to share what we know about the Incident.

What Happened?

On October 15, 2020, we were provided notification by BigCommerce, our ecommerce platform vendor, of the presence of unknown code that may have impacted the Headsweats.com website. We immediately began investigating the matter; however, the code was not made available to us by BigCommerce until February 2021. Once provided to us, we confirmed that from October 10, 2020 and October 15, 2020, the code may have copied our customers' information, including names, addresses, and credit card details. Our investigation revealed that the Incident may have involved your Information.

What Information Was Involved?

It is important to note that only limited Information about you was involved: your name, address, and credit card details. No other information about you was involved or is at risk. We have no evidence that any of the Information has been misused.

What We Are Doing.

We immediately investigated the matter, confirmed the unknown code was removed, changed passwords, retained national data security experts, and continue to implement appropriate measures to further improve the security of our systems and practices. We are working with a leading national data security firm to aid in our investigation and response and will report this Incident to relevant state authorities, as required. We also implemented additional security protocols designed to protect our systems and personal information.

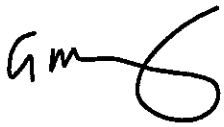
What You Can Do.

It is always recommended that you regularly review account statements and report any suspicious activity to financial institutions. Please also review the enclosed "Additional Resources" section included with this letter, which describes additional steps you can take to help protect your Information.

For More Information.

If you have any questions please call (720) 466-5098, Monday through Friday, from 9:00 a.m. to 5:00 p.m. Mountain Time (excluding some U.S. national holidays).

Sincerely,



Mike McQueeney

President
Headsweats
6525 Gunpark Dr.
Suite 370, #271
Boulder, CO 80301

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

Reporting of identity theft and obtaining a police report.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.