netrition.com
The Internet's Premier Nutrition Superstore!™

25 Corporate Circle, Suite 118
Albany, NY 12203

RECEIVED
OCT 22 2018
CONSUMER PROTECTION

October 15, 2018

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

Dear Attorney General,

We were recently notified by Shopper Approved of a potential security incident. Attached is the letter we mailed to our customers detailing the incident on 10/15/18. There were six potential New Hampshire customers affected.

If you have any questions, I can be reached at 518-456-9660.

Sincerely,

Terry Minissale
Vice President

Notice of Potential Security Incident

Netrition, Inc recently became aware of a potential security incident possibly affecting the personal information of certain customers. We are providing this notice to inform you of the incident and to call your attention to some steps you can take to help protect yourself.

What Happened

We were informed of a potential incident by Shopper Approved, LLC, a third party that provides rating and review services to Netrition.com. Members of a hacking group modified a piece of code linked to the Shopper Approved seal, an image that we display on our website. This modified computer code was designed to capture information entered on certain pages on our website. The modified code was active on our website between 12:35 a.m. EDT (4:35 UTC) on September 15, 2018, and 11:00 a.m. EDT (15:00 UTC) on September 17, 2018.

What Information Was Involved

We believe that the incident may have affected certain personal information, including information such as name, address, and possibly credit card information.

What Shopper Approved Is Doing

Upon learning of this incident, Shopper Approved promptly launched an investigation and remediated the code to remove the malicious script that was able to capture information on our website. Shopper Approved also engaged a leading cybersecurity investigation firm to assist with the company's investigation, and is continuing to review and enhance the company's security measures to help prevent something like this from happening again in the future. Shopper Approved also contacted law enforcement and will continue to cooperate with any investigation of this incident.

What You Can Do

We advise that you change your customer password on our site as a precautionary measure.

We want to make you aware of steps you can take to guard against fraud or identity theft. 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, and file a police report for identity theft and get a copy of the report. You may need to give copies of the police report to creditors to clear up your records.

You may choose to notify your bank to see if there are any additional protections available to prevent someone from accessing your account or initiating transactions without your permission. As a general practice, you can regularly monitor your accounts for unusual activity or any transactions you do not recognize. If you find anything unusual, contact your bank immediately.

You may also carefully review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not recognize, you should immediately notify the issuer of the credit or debit card as well as the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal

Trade Commission ("FTC"). In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

Other Important Information

We have included the "Information about Identity Theft Protection" reference guide, below, that describes additional steps that you may take to help protect yourself, including recommendations by the FTC regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

INFORMATION ABOUT IDENTITY THEFT PROTECTION

Review Accounts and Credit Reports: As a general precaution, you can 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 of the three national credit reporting agencies listed at the bottom of this guide.

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 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 protecting 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.

For residents of Rhode Island You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.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 at the bottom of this page.

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.

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. 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 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 remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
(2) proper identification to verify your identity;
(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
(4) payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone. A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.(By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.) You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

More Information about Fraud Alerts and Credit Freezes: You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies' Contact Information

Equifax (www.equifax.com)

General Contact:
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374

Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)

General Contact:
P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)

General Contact:
P.O. Box 105281
Atlanta, GA 30348
800-888-4213

Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872

FAQ

What Happened?

We recently learned of a potential security incident from Shopper Approved, LLC, a company that provides rating and review software on our website. A hacking group managed to gain access to and modify code of a Shopper Approved feature that we use on our website. The modified code was designed to capture payment card data and other information entered on certain web pages, and affected some of our users between 12:30 a.m. (Eastern) on Saturday, September 15, 2018 and 2:00 p.m. (Eastern) on Monday, September 17, 2018.

What information was affected?

The following types of information that you provided during this time period may have been collected: name, address, and possibly credit card information.

How did this happen?

Shopper Approved has hired a leading cybersecurity investigation firm to learn how the hacking group was able to modify the code. This investigation is ongoing.

What is Shopper Approved doing?

Shopper Approved promptly responded to this matter by disabling the malicious code and engaging a leading cybersecurity firm to assist with the investigation. Shopper Approved also contacted law enforcement about this incident, is monitoring its systems, and is working to review and enhance security measures to help prevent something like this from reoccurring.

What should I do?

We advise that you change your customer password on our site as a precautionary measure.

If you were informed that your payment card data may have been affected, you can review your credit and debit card account statements as soon as possible to look for any transactions that you do not recognize, and continue to monitor your statements for unusual activity going forward. If you see anything you do not recognize, immediately notify the issuer of the credit or debit card. Cardholders are typically not held responsible for any fraudulent activity reported in a timely fashion.

Additional steps and best practices are included with the "Information About Identity Theft Protection Guide" included with the notice you received.

What new security measures are being implemented to help prevent this from happening again?

In addition to removing the malicious code in the feature on our website that was capturing information, Shopper Approved has taken steps to secure the code from future misuse. Shopper Approved is working with a leading cybersecurity investigation to firm to monitor systems and is continuing to enhance security measures.