Cooley

Randy V. Sabett
+1 202 728 7090
rsabett@cooley.com

October 16, 2019

Attorney General Bob Ferguson
Washington Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Dear Attorney General Ferguson:

We are writing to inform you that on September 11, 2019, our client Nutraceutical Wellness Inc. dba Nutrafol ("Nutrafol") became aware of the initial signs that Nutrafol was experiencing a security incident and may have been the victim of a criminal cyber security attack. Through a forensics examination it was revealed that customer personal information, including credit card information, name, and address may have been accessed. There were 518 Washington residents affected.

Please be assured that Nutrafol is taking this matter very seriously. The company has been working diligently to investigate the unauthorized activity and remediate the method of unauthorized access. Upon discovering this unauthorized activity, the company began working with a nationally recognized computer security firm to conduct an investigation into the extent of this unauthorized activity. Through our acquiring bank, the credit card companies have been notified and provided with the affected credit card numbers so they can notify the banks that issued the affected credit cards.

Nutrafol sent the attached notification letter to the affected customers on October 11, 2019. Please feel free to contact me at **202-728-7090** or rsabett@cooley.com if you have any questions.

Cooley LLP

Randy V. Sabett

Enclosure

Nutraceutical Wellness Inc. dba Nutrafol

Return Mail Processing Center
[ ]
[ ]

<<Name 1>><<Name 2>><<Name 3>><<Name 4>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

Dear <<Name 1>>:

NOTICE OF DATA INCIDENT

We are writing to inform you of a potential security incident involving Nutraceutical Wellness Inc., dba Nutrafol ("Company"). While all details have not yet been confirmed, we are providing this notice as a precaution for potentially affected individuals and to call your attention to some steps you can take to help protect your personal information. We sincerely regret any concern this may cause you.

What Happened

We became aware on September 11, 2019 that Company may have been the victim of a cybercrime. As a result of a security incident, some of your data may have been accessed by an unauthorized third party. We have been working closely with a nationally recognized computer security firm to investigate this. While the investigation is ongoing, we have taken initial steps to address the incident and prevent this from happening again.

What Information Was Involved

The information that may have been accessed by an unauthorized third party includes names, addresses, and credit card information. Based on our investigation, your information could be affected by this incident. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing

We take the privacy of personal information very seriously and we are committed to maintaining the security, confidentiality, and integrity of all data and information that we handle. We took steps to address this incident promptly after it was discovered, including initiating an internal investigation and retaining a nationally recognized computer security firm to assist us in our investigation and respond to this incident. To help prevent this type of incident from reoccurring in the future, we are continuing to review and enhance security measures moving forward.

What You Can Do

Although we are not aware of any misuse of your information arising as a result of this incident, we want to provide you with steps that you can take as a precaution:

- **Checking Credit Reports and Financial Accounts.** Check your personal 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. 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 it. You may need to give copies of the police report to creditors to clear up your records. You can also review your financial account statements to determine if there are any discrepancies or unusual activity listed. If you see anything you do not understand, call the financial institution

- **Reviewing credit and debit card account statements.** If your credit or debit card numbers may have been affected, you may also wish to review credit and debit card account statements to determine if there are any discrepancies or unusual activity listed. We urge individuals to remain vigilant and continue to monitor statements for unusual activity going forward. If you see something you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should notify the issuer of the credit or debit card. 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.

- **Reviewing Explanation of Benefits Documents.** You can also review explanation of benefits statements that you receive from your health insurer or health plan or review for persons whose medical bills you assist with or pay (such as your child). If you identify services listed on the explanation of benefits that were not received, please contact your insurer or health plan.

- **Consulting the Identity Theft Protection Guide.** Finally, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact us at +1 (888) 320-0385 between the hours of 9 am to 5 pm Eastern time, Monday through Friday. Again, we sincerely regret any concern this incident may cause.

Sincerely,

Giorgos Tsetis
Chief Executive Officer

INFORMATION ABOUT IDENTITY THEFT PROTECTION

Review Accounts and Credit Reports: 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 or more of the three national credit reporting agencies listed at the bottom of this page.

You should 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 protection 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.

Security Freezes and Fraud Alerts: You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 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.

For more information, including information about additional rights, you can visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf, https://www.consumerfinance.gov/learnmore/, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

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 and Security Freezes:
P.O. Box 740256, Atlanta, GA 30374

Experian (www.experian.com)
General Contact:
P.O. Box 2002, Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9556, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact, Fraud Alerts and Security Freezes:
P.O. Box 2000
Chester, PA 19022
888-909-8872