February 23, 2017

Benjamin A. Powell

+1 202 663 6770 (t)
+1 202 663 6363 (f)
benjamin.powell@wilmerhale.com

VIA EMAIL AT SECURITYBREACH@ATG.WA.GOV

Attorney General Bob Ferguson
Office of the Attorney General
Washington State
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Incident Notification

Dear Attorney General Ferguson:

On February 6, 2017, our client, Abbott Nutrition ("Abbott" or the "Company"), was first alerted of a security incident at Aptos, Inc. ("Aptos"), a third-party service provider that provided and managed the e-commerce platform for AbbottStore.com. We understand that Aptos may notify you separately regarding this incident. This notice refers to the same underlying incident, which may affect Abbott customers who purchased products from AbbottStore.com. Aptos retained the services of an outside security forensics team to investigate the nature and scope of the incident. Aptos has also shared information with law enforcement.

Aptos' investigation determined that an unauthorized party entered Aptos' systems and was able to access and possibly obtain the following information for customers who purchased products from AbbottStore.com from approximately June 2013 to December 2016: names, addresses, phone numbers, e-mail addresses, payment card numbers, and expiration dates. Additionally, for customers who placed an order on AbbottStore.com between approximately April 11 and August 8, 2016 and between approximately November 12 and November 28, 2016, the information compromised may also have included card security codes (CVV numbers). Individuals who visited AbbottStore.com but did not make a purchase online or by phone are not affected. Approximately 1,819 individuals with billing addresses in the state of Washington were potentially affected.

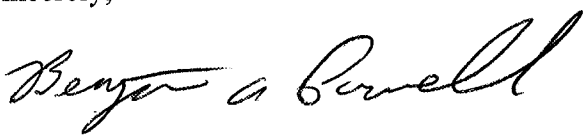
The unauthorized party never had access to Abbott's systems. Out of an abundance of caution, Abbott has disabled AbbottStore.com's website order function and is in the process of moving to a new system to process orders from AbbottStore.com. During this transition, customers can purchase most of Abbott's products from other retailers online. The Company has set up a "Where to Buy" tool on AbbottStore.com to assist.

Abbott is notifying all customers who purchased products from AbbottStore.com who may have been affected by this incident. Abbott has retained AllClear ID to protect affected individuals' identities for 12 months at no cost. To comply with Abbott's obligations under the state and

territorial data breach notification laws, on February 23, 2017, the Company will be mailing notification letters to all affected customers in substantially the same form as the enclosed letter. *See* Wash. Rev. Code § 19.255.010(1).

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Benjamin A. Powell

Enclosure

ABBOTT NUTRITION

3300 STELZER ROAD • COLUMBUS, OHIO 43219-3034

February 24, 2017

NOTICE OF DATA BREACH

Dear Customer:

We wanted to notify you of an unauthorized intrusion which resulted in the compromise of some customer information at AbbottStore.com. The privacy and protection of our customers' information is a matter we take very seriously, and we have worked swiftly to resolve the incident. We recommend that you closely review the information provided in this letter for some steps that you may take to protect yourself against potential misuse of your information.

What Happened?

On February 6, 2017, we were first alerted of a security incident at Aptos, Inc. (Aptos), the company that provided and managed the e-commerce platform for AbbottStore.com. This incident may affect our customers who purchased products from AbbottStore.com. Aptos retained the services of an outside security forensics team to investigate the nature and scope of the incident.

What Information Was Involved?

Aptos' investigation determined that an unauthorized party entered Aptos' systems and was able to access and possibly obtain the following information for customers who purchased products from AbbottStore.com from approximately June 2013 to December 2016: names, addresses, phone numbers, e-mail addresses, payment card numbers, and expiration dates.

Additionally, for customers who placed an order on AbbottStore.com between approximately April 11 and August 8, 2016 and between approximately November 12 and November 28, 2016, the information compromised may also have included card security codes (CVV numbers).

Individuals who visited AbbottStore.com but did not make a purchase online or by phone are not affected.

What We Are Doing

Your trust is a top priority for Abbott, and we deeply regret any inconvenience this may cause. There is nothing more important to us than our customers. We conducted a thorough review of the potentially affected records. Aptos has also shared information with law enforcement.

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

- AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call [redacted] and a dedicated investigator will help recover financial losses, restore your credit, and make sure your identity is returned to its proper condition.

- AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. To enroll with AllClear Identity Credit Monitoring, go to [redacted] or call the phone number above. Again, we apologize for any inconvenience caused by this incident.

What You Can Do

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission (FTC) or law enforcement, such as your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
https://www.identitytheft.gov/

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take these additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently; and (2) file and keep a copy of a local police report as evidence of the identity theft crime.

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain credit reports from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you should request that the credit reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by

going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting bureaus to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days.

Also, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report. A security freeze prohibits a credit reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. The credit reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. You may be charged to place or lift a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide credit reporting agencies at:

Equifax P.O. Box 105788 Atlanta, GA 30348 (800) 525-6285 www.equifax.com	Experian P.O. Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19016 (800) 680-7289 www.transunion.com

For More Information

Again, we apologize for any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance, please do not hesitate to visit [redacted] or contact our call center at [redacted] Our call center will be available 9 a.m.-9 p.m. ET through March 5, 2017, and 9 a.m.-6 p.m. ET Monday-Saturday beginning on March 6, 2017.

Sincerely,

Roger M. Bird
President, U.S. Nutrition
AbbottStore

IF YOU ARE AN IOWA RESIDENT:
You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

IF YOU ARE A MARYLAND RESIDENT:
You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

IF YOU ARE A NORTH CAROLINA RESIDENT:
You may obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.gov

IF YOU ARE AN OREGON RESIDENT:
You may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(503) 378-4400
http://www.doj.state.or.us/