



945 East Paces Ferry Rd., Suite 1475, Atlanta, GA 30326
+1-866-493-7037 aptos.com

RECEIVED

APR 10 2017

**OFFICE OF CONSUMER PROTECTION
INVESTIGATIONS**

April 4, 2017

BY U.S. MAIL

Office of Consumer Protection
Department of Commerce and Consumer Affairs
Leiopapa A. Kamehameha Building
235 South Beretania Street, Suite 801
Honolulu, Hawaii 96813

To Whom It May Concern:

Referring to our previous letter dated February 25, 2017, and consistent with Haw. Rev. Stat. Ann, § 487N-2, this letter provides supplemental notice on behalf of an additional Retailer. This Retailer is notifying a total of 1,302 Individual Consumers with billing addresses in Hawaii. Please see the attached schedule and consumer notice for further details.

Aptos is committed to full cooperation in answering any questions that your office may have. Please feel free to contact me with any questions at securityinfo@aptos.com.

Respectfully yours,

/s/

David Baum
Senior Vice President, General Counsel

Enclosures

Schedule

Retailer Name	Nutrex Hawaii, Inc.
Contact Information	73-4460 Queen Ka'ahumanu Hwy. #102 Kailua-Kona, HI 96740 Jim Crum, IT Director 808-329-4677 jcrum@cyanotech.com
Number of Individual Consumers Notified in This Jurisdiction	1,168 [Retailer notes that, based upon communications from Aptos, no PIN or CVV or SSN data for its customers]
Date Individual Consumers Notified	2/24/2017
Form of Individual Consumer Notification	Mail

[Insert Nutrex Hawaii.JPG]

[DATE]

[ADDRESS]

Dear [NAME],

Nutrex Hawaii recently became aware of a potential security incident possibly affecting the personal information of certain individuals who made a payment card purchase on the Nutrex-Hawaii.com website. We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened

We were recently informed by the company that hosts and operates our website of a potential security incident involving our website. Based upon the vendor's forensic investigation, it appears that an unauthorized individual was able to gain access to portions of our website and install malicious software on the website servers that was designed to capture payment card information.

What Information Was Involved

We believe that the incident could have affected certain information (including name, address, email address, telephone number, payment card account number, and expiration date) of individuals who made a purchase on the website. According to our records, you made a payment card transaction on the website so it's possible that your information may be affected. Please note that because we do not collect sensitive personal information like Social Security numbers, this type of sensitive information was not affected by this incident.

What We Are Doing

We take the privacy of personal information seriously, and deeply regret that this incident occurred. We've taken steps to address this incident promptly after we were alerted to it, including communicating with the vendor that hosts and operates the website to learn more about what occurred. The vendor informed us that they have engaged an outside forensic investigation firm to assist them in investigating and that the vendor and forensic firm are remediating the situation by removing the malware, and deploying file monitoring software and an endpoint security program to enhance the security of all the websites that they host and operate. While both we and the vendor are continuing to review and enhance security measures, the incident has now been contained. In addition, the incident has been reported to federal law enforcement and the vendor is cooperating with their investigation.

What You Can Do

We recommend that you 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.

Although Social security numbers were not at risk in this incident, we recommend, as a general practice, that you 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. As an additional precaution, we are providing information and resources to help individuals protect their identities. This includes an "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

For More Information

For more information about this incident, or if you have additional questions or concerns about this incident, you may contact us toll free at 844-749-5105 between 9am and 9pm Eastern Time, Monday through Friday. Again, we sincerely regret any concern this event may cause you.

Sincerely,

[Insert GerryC.JPG]

Gerald R. Cysewski, Ph.D.

President and CEO

Information about Identity Theft Protection

Review Accounts and Credit Reports: You should 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 also 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>.

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.

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
877-322-8228

Fraud Alerts and Security Freezes:

P.O. Box 2000, Chester, PA 19022
888-909-8872

aptos

945 East Paces Ferry Rd., Suite 1475, Atlanta, GA 30326
+1-866-493-7037 aptos.com

RECEIVED

17 FEB 28 AIO :46

STATE OF HAWAII
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS

February 25, 2017

BY U.S. MAIL

Office of Consumer Protection
Department of Commerce and Consumer Affairs
Leiopapa A. Kamehameha Building
235 South Beretania Street, Suite 801
Honolulu, Hawaii 96813

To Whom It May Concern:

Consistent with Haw. Rev. Stat. Ann, § 487N-2, this letter provides notice of a computer data security incident. Aptos, Inc. (“Aptos”) contracts with a number of online retailers (“Retailers”) who in turn do business with their Consumers (“Individual Consumers”). Aptos provides a digital commerce platform that functions as the back-end for the Retailers’ online stores, as well as an order management system utilized by certain Retailers. As a result, Aptos holds the data of Individual Consumers associated with their transactions at a number of online stores operated by various Retailers.

Aptos has determined that there has been remote access intrusion to its systems that resulted in unauthorized access to information of Individual Consumers. Aptos provides this notice on behalf of those Retailers on the attached schedule. For those Retailers, the intrusion resulted in access to online transaction data including Individual Consumers’ first and last names, addresses, phone numbers, payment card numbers, and expiration dates. In certain instances, CVV2s may have been exposed.

Each Retailer has determined the number of Individual Consumers in your state to whom it will send notice. The number of Individual Consumers receiving notice from each Retailer is listed on the attached schedule, along with contact information for each Retailer and information about the Retailer’s distribution of notices to Individual Consumers.

Our investigation indicates that the intrusion began in approximately February 2016 and ended in approximately December 2016. The Retailers on the attached schedule are notifying a total of 3,002 Individual Consumers with billing addresses in Hawaii.

Aptos discovered indications of this intrusion in late November 2016, and promptly reported this matter to the FBI and the U.S. Department of Justice. Law enforcement requested that Aptos not notify the Retailers before February 5, 2017. Aptos gave notice to affected Retailers on February 6, and thereafter provided Individual Consumer contact information to affected Retailers. We are unaware of any reports of payment card fraud or other misuse of the data at issue.

In response to these events, Aptos has worked with a leading cybersecurity firm to remove the malware from its systems and to make security updates to the systems; including strengthening access controls.

Aptos is committed to full cooperation in answering any questions that your office may have. Please feel free to contact me with any questions at securityinfo@aptos.com.

Respectfully yours,

/s/

David Baum
Senior Vice President, General Counsel

Enclosures