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

February 25, 2017

BY U.S. MAIL

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

To Whom It May Concern:

Consistent with Wash. Rev. Code Ann. § 19.255.010, 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 7,395 Individual Consumers with billing addresses in Washington.

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

Schedule

Retailer Name	Alpha Industries
Contact Information	14200 Park Meadow Drive, Suite 110S Chantilly, VA 20151 Stephanie Cohen 703-378-1420 ext. 138 stephanie@alphaindustries.com
Estimated Number of Individual Consumers Notified in This Jurisdiction	1,013 [Retailer notes that, as to its customers, no PIN or CVV or SSN data was exposed]
Anticipated Date Individual Consumers Notified	Planned for week of 2/27/2017
Form of Individual Consumer Notification	Mail

Retailer Name	Atlantic Cigar
Contact Information	c/o Davis Wright Tremaine LLP 1919 Pennsylvania Ave. NW, Suite 800 Washington, DC 20006 Christin McMeley Davis Wright Tremaine 202-973-4264 christinmcmeley@dwt.com
Number of Individual Consumers Notified in This Jurisdiction	849 [Retailer notes that, as to its customers, no PIN or CVV or SSN data was exposed]
Date Individual Consumers Notified	On or about 3/1/2017
Form of Individual Consumer Notification	Mail

Retailer Name	Bluemercury, Inc.
Contact Information	1010 Wisconsin Ave. NW, #700 Washington, District of Columbia 20007 Jennifer Dimotta 202-355-6000 jdimotta@bluemercury.com
Number of Individual Consumers Notified in This Jurisdiction	778 [Retailer notes that, as to its customers, no PIN or CVV or SSN data was exposed]
Date Individual Consumers Notified	Email Notice: 02/15/17 Statutory Letter Notice: 02/21/17
Form of Individual Consumer Notification	By mail and/or email, depending on available contact information for consumer

Retailer Name	Century, LLC
Contact Information	1000 Century Blvd. Oklahoma City, OK 73110 Mike Maloney 405-426-4281 mmaloney@centurymartialarts.com
Number of Individual Consumers Notified in This Jurisdiction	639 [Retailer notes that, as to its customers, no PIN or CVV or SSN data was exposed]
Date Individual Consumers Notified	2/19/2017
Form of Individual Consumer Notification	Email

Retailer Name	Movie Mars, Inc.
Contact Information	2024 Independence Commerce, Suite E Matthews, NC 28105 Brian Marzano 704-628-7770 brian.m@moviemars.com
Number of Individual Consumers Notified in This Jurisdiction	524
Date Individual Consumers Notified	TBD
Form of Individual Consumer Notification	Mail

Retailer Name	New England Biolabs, Inc.
Contact Information	240 County Line Rd. Ipswich, MA 01938 Sharon Kaiser, CIO, Director of IT 978-380-7576 ITInfo@neb.com
Number of Individual Consumers Notified in This Jurisdiction	746
Date Individual Consumers Notified	2/17/2017
Form of Individual Consumer Notification	Email

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	725 [Retailer notes that, based upon communications from Aptos, no PIN or CVV or SSN data for its customers was exposed]
Date Individual Consumers Notified	2/24/2017
Form of Individual Consumer Notification	Mail

Retailer Name	Plow and Hearth, LLC
Contact Information	7021 Wolftown-Hood Road Madison, VA 22727 Leslie Newton, COO 540-948-2272 lnewton@plowandhearth.com
Number of Individual Consumers Notified in This Jurisdiction	1,274 [Retailer notes that based upon communications from Aptos, no PIN or SSN data for its customers was exposed]
Date Individual Consumers Notified	Between 2/27/17 and 3/14/17
Form of Individual Consumer Notification	Mail

Retailer Name	Vapour Organic Beauty, LLC
Contact Information	P.O. Box 99 Taos, NM 87571 Krysia Boinis (owner) Terecina Romero (IT DEPT) 575-737-0732 / 575-751-3662 krysia@vapourbeauty.com terecina@vapourbeauty.com
Number of Individual Consumers Notified in This Jurisdiction	847 [Retailer notes that, as to its customers, no PIN or CVV or SSN data was exposed]
Date Individual Consumers Notified	TBD
Form of Individual Consumer Notification	Email and mail

ALPHA INDUSTRIES

14200 Park Meadow Drive, Suite 110S
Chantilly, VA 20151
Tel: 703-378-1420
Fax: 703-378-4910

[Customer name]
[Customer address]
[City, State, Zip]

Notice of Data Breach

Dear [Customer name]:

We write to inform you of an incident involving access to information associated with online purchases made on our website www.alphaindustries.com and www.shopalphaindustries.com which resolves to www.alphaindustries.com. Although we are unaware of any actual misuse of your information, we are providing notice to you and other potentially affected customers about the incident, and about tools you can use to protect yourself against possible identity theft or fraud.

What Happened?

We were informed on February 6, 2017 that our website www.alphaindustries.com experienced an intrusion last year. Our site is operated for us by a third-party platform provider, Aptos, and it was Aptos that experienced the intrusion.

To date, the investigation indicates that the intrusion began in approximately February 2016 and ended in December 2016. The intruder(s) placed malware on Aptos' servers, and by doing so gained access to our customers' payment card data, including payment card numbers. The intruder(s) also had access to historical payment card data. Because you have provided your payment card information to us in the past, we are notifying you about this data breach.

You may wonder why you are hearing about the breach now. Aptos did not discover the breach until November 2016. In addition, law enforcement is investigating, and asked that notification to customers be delayed to allow the investigation to move forward.

What Information Was Involved?

The information that the intruder(s) had access to includes your first and last name, your address, your phone number, email address and any debit or credit card numbers with expiration dates you may have used on our website. To date, no security codes, CVV codes, PIN numbers, social security numbers, passwords, or any other personal identification numbers involving our customer information was accessed.

What Are We Doing?

Aptos has worked with a leading cybersecurity firm to remove the malware from its systems and is actively monitoring the platform to safeguard personal information.

Aptos has also contacted and offered its cooperation to federal law enforcement, and steps were taken to supply the numbers of affected cards to their issuers for monitoring. Also, even though this incident did not involve security codes, CVV codes, PIN numbers, social security numbers, passwords, or any other personal identification numbers, we are offering complimentary credit monitoring and an identity theft protection product by Equifax to help alleviate any concerns you may have.

What You Can Do.

To protect yourself from the possibility of identity theft, we recommend you immediately contact your credit or debit card company and inform them that your card information may have been compromised, so that they can issue you a replacement card. While we do not believe there has been any actual misuse of your information, we suggest you remain vigilant and review your banking and card statements as well as credit reports, and report any suspicious activity to the relevant financial institution.

You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. You can also contact these sources about steps you can take to avoid identity theft.

Your state attorney general can be contacted at [phone number, address, and website].

To contact the FTC and file a complaint, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

You can also contact one of the three major credit bureaus to monitor your credit report for any suspicious activity. You should immediately notify the credit bureaus if your credit reports show anything suspicious. The credit bureau can be contacted as follows:

Experian (888) 397-3742 www.experian.com/fraud	Equifax (888) 766-0008 www.alerts.equifax.com	TransUnion (800) 680-7289 https://fraud.transunion.com

As a precautionary measure to help better protect your credit file from potential misuse, we have partnered with Equifax ® to provide its Credit Watch ™ Silver credit monitoring and identity theft protection product for one year at no charge to you.

If you choose to take advantage of this Equifax Credit Watch Silver product, it will provide you with a notification of key changes to your Equifax credit file, up to $25,000 Identity Theft Insurance Coverage, automatic fraud alerts, access to your Equifax credit report and Identity Restoration. To enroll in Equifax Credit Watch Silver, you may sign up online at www.myservices.equifax.com/silver. You must complete the enrollment process for Equifax Credit Watch Silver by June 1, 2017.

Even if you decide not to take advantage of this offer, you may still receive Equifax Identity Restoration in the event that you become victim of identity theft by calling 877-xxx-xxxx, 9:00 a.m. to 8:00 p.m. EST, Monday through Friday, before March 1, 2018.

For More Information

We at Alpha Industries take the security of our customer information very seriously and truly regret any inconvenience that this incident may have caused you.

If you have any questions about this incident or any of the products we are making available to you, please call 844-xxx-xxx Monday through Friday from 9:00 a.m. to 9:00 p.m. EST.

We thank you for your patronage, your understanding and your patience.

Sincerely,

Colin Israel
COO and CFO

3 Horne Drive Suite 102
Folcroft, PA 19032
844-371-5335
10 a.m. – 5:30 p.m. EST daily

[Date]

«First_name» «Last_name»
«Address_1», «Suite/Apt»
«City», «State» «Zip»

NOTICE OF DATA BREACH

Dear «First_name» «Last_name»,

We are writing to notify you about a security incident that involves your payment card information.

What Happened? We use a third party service provider, Aptos, to maintain our database of customer ordering information. In November 2016, Aptos discovered indications that its systems had been compromised and promptly reported its suspicions to U.S. law enforcement agencies, who requested Aptos delay any notification of the incident to third parties, including Atlantic Cigar Co., during the criminal investigation. On February 10, 2017, Aptos notified us that there had been remote access intrusion to Aptos' systems that resulted in unauthorized access to our customers' information. At this time, we are unaware of any reports of credit card fraud or other misuse of our customers' data.

What Information Was Invloved? The intrusion resulted in access to online transaction data, including your first and last name, billing and shipping address(es), phone number, payment card information including account number and expiration date.

What We Are Doing. In response to these events, Aptos has worked with a leading cybersecurity firm to remove the malware from and update the security of its systems, including strengthening access controls. Additionally, Atlantic Cigar Co. has 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 13 months:

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call «DID_Phone» 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. You may sign up online at enroll.allclearid.com using the following redemption code: {Redemption_Code}.

Additional steps may be required by you in order to activate your phone alerts and monitoring options.

Other Important Information. Please review the "Further Steps and Contact List" information on the reverse side of this letter which identifies additional steps to take to protect your information.

For More Information. If you have further questions or concerns about this incident, please call AllClear ID, Monday through Saturday, 8 a.m. – 8 p.m. CST.

We take all privacy and security incidents seriously. We deeply regret any inconvenience this may cause you, and thank you for your understanding.

Sincerely,

Paul Scipioni
President

(see reverse side)

FURTHER STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION
CONTACT LIST

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	annualcreditreport.com

Fraud Alert

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

We will **NOT** send you any electronic communications regarding this incident and ask you to disclose any personal information.

bluemercury, inc.

NOTICE OF DATA BREACH

February 22, 2017

On behalf of Bluemercury, I am writing to inform you about a recent incident involving unauthorized access of personal information about you. You may have received this information via an email. We regret that this incident occurred and appreciate your time to read this letter.

WHAT HAPPENED?

On February 7, 2017, we were informed that Aptos, our former digital platform provider, experienced a security incident last year that involved certain of its retail customers' websites, including www.bluemercury.com. Aptos has indicated intrusions to some of their systems began in February 2016 and ended in December 2016. During that time, we understand that cyber criminals placed malware on Aptos' servers and gained unauthorized access to Bluemercury's data. Although we ended our relationship with Aptos in September 2016, we have been assured that the malware has been removed and that the criminals no longer have access to their systems or data.

Aptos did not discover the intrusion until November 28, 2016. We understand that Aptos contacted Federal law enforcement agencies and the U.S. Department of Justice at that time. We also understand that Aptos was requested by law enforcement to delay notifying its retailer customers, including Bluemercury, so as not to interfere with their ongoing investigation. We also understand that law enforcement continues to investigate this incident.

WHAT INFORMATION WAS INVOLVED?

Aptos has informed us that attackers had access to data associated with approximately 54,000 client orders made before September 12, 2016 to include: First and Last Name; Address; Phone Number; Email; Address; and Debit or Credit Card Number with expiration dates. Aptos has indicated that no Credit Verification Values (CVV) or Social Security Numbers (SSN) associated with Bluemercury clients were retained or accessed.

WHAT ARE WE DOING?

We ended our relationship with Aptos in September 2016 for unrelated reasons. We have been working with Aptos to learn more about the incident. Aptos has indicated it retained a leading cybersecurity firm to remove the malware from its systems and is actively monitoring the platform to safeguard information. We have instructed Aptos to destroy any and all remaining Bluemercury client data.

WHAT CAN YOU DO?

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring credit reports. We recommend you immediately contact your credit or debit card company and inform them that your card information may have been compromised. Your bank or credit card provider will suggest appropriate steps to protect your account. You should review your bank and card statements regularly, and immediately report any suspicious activity to your bank or credit card provider. Payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner.

We at Bluemercury value our client relationship, appreciate your business and would like to provide as much assistance as we can. Just like it is a good practice to monitor your bank accounts, it is a good practice to monitor your identity. Therefore, as an additional service for our clients, we have arranged to have AllClear ID (www.allclearid.com) provide identity protection support for 12 months at no cost to you. AllClear ID's Identity Repair services are available to you starting on the date of this notice and can be used at any time during the next 12 months. This service is automatically available to you with no enrollment required. As you monitor your credit, if you spot a problem, simply call AllClear ID at 1-855-336-6688, provide your Reference Code {Reference_Code} and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

CONTACTING THE FEDERAL TRADE COMMISSION, LAW ENFORCEMENT & THE CREDIT BUREAUS

In addition, you may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.consumer.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, 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 may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 916-8800
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
www.equifax.com	www.experian.com	Chester, PA 19022
		www.transunion.com

You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. 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. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. 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. In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze to restrict access to your credit report:

(1) Equifax – (800) 349-9960
(2) Experian – (888) 397-3742
(3) TransUnion – (888) 909-8872

You will need to supply your name, address, date of birth, Social Security number and other personal information. The fee to place a credit freeze varies based on where you live. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

FOR MORE INFORMATION

We regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact our support agents for this event at 1-855-336-6688 if you have any questions or concerns.

Sincerely,

Bernard Locraft

Bernard F. Locraft,
Corporate Controller
Bluemercury, Inc
1010 Wisconsin Ave NW, #700,
Washington, District of Columbia 20007

ADDITIONAL INFORMATION FOR SOME STATES

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. You can contact the Iowa Attorney General at:

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
http://www.iowaattorneygeneral.gov/

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

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

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

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

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

IF YOU ARE A RHODE ISLAND RESIDENT: Please contact state or local law enforcement to determine whether you can file or obtain a police report in regard to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400
http://www.riag.ri.gov/

NOTICE OF DATA BREACH

Dear Customer:

Century was informed on February 8th, 2017 by our 3rd Party Ecommerce Provider (Aptos) that their software platform which hosts centurymartialarts.com experienced a data breach. The investigation by Aptos and the FBI Cyber Crimes Division indicates the intrusion began in February 2016 and ended in December 2016. During this time the attackers gained access to customer information. To date we have no confirmation that any card or personal data has been misused. As a precautionary step Aptos worked with law enforcement to provide the numbers of the affected cards to the issuers for additional security monitoring.

What Information Was Involved?

The information the attacker had access to was first and last name, address, phone number and any credit or debit card numbers with expiration dates.

What Is Being Done To Secure The Platform?

Our 3rd Party Provider hired Mandiant, a leading cybersecurity firm, which completed the removal of the malware from their servers and continues to actively monitor their platform to safeguard personal information going forward. Aptos is also fully cooperating with federal law enforcement in an effort to bring to justice the perpetrator.

What We Recommend To Our Customers:

To protect yourself from the possibility of identity or credit card theft we recommend you immediately contact your credit or debit card company and inform them that your card information may have been compromised so they can issue you a replacement card. Also please review your banking and credit card statements and report any suspicious activity to the relevant financial institutions.

Century's Promise To Our Customers

We deeply regret this breach occurred despite the many security safeguards which are in place. Once again we have been assured by Aptos that this issue has been resolved and our site is secure for future transactions.

We are committed to secure your personal information by holding our vendors to the highest business standards.

For Questions Or More Information

If you have any questions or if we can assist you in any way, please call 1-877-272-1902 Monday through Thursday between the hours of 8:00 am and 5:00 pm Central Time.

Sincerely,

Paul Webb

President, Century LLC

2024 INDEPENDENCE COMMERCE AVENUE, SUITE E
MATTHEWS, NC 28105
704-628-7770

February 21, 2017

[Customer Name]
[Customer Address]
[Customer Address]

NOTICE OF DATA BREACH

Dear Customer:

We are writing to you because of an incident involving access to information associated with online purchases made on our website www.MovieMars.com. Although we are unaware of any actual misuse of your information, we are providing notice to you and other potentially affected customers about the incident, and about tools you can use to protect yourself against possible identity theft or fraud.

What Happened?

The MovieMars.com site is operated by a third-party company, Aptos, Inc. (our "platform provider"). We were informed on February 6, 2017 that the platform provider's systems experienced an intrusion last year. The intruder or intruders placed malware on the platform provider's services, and by doing so gained access to our customers' payment card data. To date, the investigation indicates that the intrusion began in approximately February 2016 and ended in December 2016. The attackers gained access to customer information including payment card numbers as customers made transactions on the platform provider's systems, and had access to historical payment card data. Because you have provided your payment card information to us in the past, we are notifying you about this data breach.

You may wonder why you are hearing about the breach now. The platform provider did not discover the breach until November 2016. In addition, law enforcement is investigating, and asked that notification to customers be delayed to allow the investigation to move forward.

What Information Was Involved?

The information that the attacker had access to includes your first and last name, address, phone number, and any debit or credit card numbers with expiration dates you may have used on our website.

What Are We Doing?

Our platform provider has worked with a leading cybersecurity firm to remove the malware from its systems and is actively monitoring the platform to safeguard personal information. Our platform provider has also contacted and offered its cooperation to federal law enforcement.

What You Can Do

Please be sure to review the enclosed "Additional Resources" section included with this letter. This section describes some additional steps you can take to help protect yourself (such as obtaining a copy of your credit report, or placing a security freeze on your credit report) and provides important contact information for the Federal Trade Commission, other law enforcement agencies, and credit reporting agencies.

In addition, we recommend you consider the following:

- **Contact Your Credit or Debit Card Issuer.** While we have taken steps to notify credit card processors, we recommend that you also immediately notify your credit card issuing bank and follow its advice with regard to your credit card.
- **Regularly Review Your Financial Statements.** We recommend you remain vigilant by regularly reviewing your credit card and bank account statements and monitoring free credit reports; and immediately alert your credit card issuing bank of any suspicious charges. This is one of the most important steps that you can take to detect and prevent any unauthorized use of your credit card number.
- **Be Aware of online "Phishing" Schemes.** You should also always be on the lookout for phishing schemes – emails where fraudsters pose as legitimate companies in order to trick people into disclosing personal information or clicking a link that causes the installation of malware. Any email correspondence we may send regarding this matter will not contain any clickable hyperlinks and will not ask you to reply with personal information. Never provide sensitive information to unsolicited requests claiming to come from us, your bank, or other organizations.

For More Information

We sincerely regret that this incident happened, and will continue to put the right measures in place to maintain the security of your information. For more information on preventing identity theft, please review the "Additional Resources" section.

ADDITIONAL RESOURCES

Obtain a Free Credit Report. We also recommend you remain vigilant by obtaining and reviewing your credit report. You may request a free copy of your U.S. credit report once every 12 months by visiting www.annualcreditreport.com or by calling 1-877-322-8228 toll free. You can print a copy of the request form at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf. You should review this for any information that is not accurate.

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Information on Credit Report Fraud Alerts. You also may place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.

	Equifax	**Experian**	**TransUnion**
Phone	1-800-525-6285 or 1-888-766-0008	1-888-397-3742	1-800-680-7289
Address	Equifax Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Credit Report Fraud Alert Form	https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp fraud/center.html	https://www.experian.com/fraud/center.html	https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp

Place a Security Freeze on Your Account. In addition to a fraud alert, you may also have a security freeze placed on your credit file. A security freeze will block a credit bureau from releasing information from your credit report without your prior written authorization. Please be aware that a security freeze may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. The fees for placing a security freeze vary by state, and a consumer reporting agency may charge a fee of up to $10.00 to place a freeze or lift or remove a freeze. To place a security freeze on your credit report, you may send a written request to **each** of the major consumer reporting agencies by regular, certified, or overnight mail. You can also place security freezes online by visiting **each** consumer reporting agency online.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. 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:

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. 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). 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.

	Equifax	**Experian**	**TransUnion**
Address	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp	https://www.experian.com/freeze/center.html	https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp

Contact Law Enforcement.

If you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency, your state's attorney general, or the Federal Trade Commission.

Federal Trade Commission. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. You can also call 1-877-ID-THEFT (877-438-4338) or write to Federal Trade Commission at 600 Pennsylvania Avenue, NW, Washington, DC 20580 for additional guidance. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcement for their investigations.

State-Specific Information.

For residents of Maryland, North Carolina, and Rhode Island: For information on how to avoid identity theft or to contact your state's attorney general, please use the below information.

For residents of Massachusetts and Rhode Island: Under Massachusetts and Rhode Island laws, you have the right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

	Maryland Attorney General	**North Carolina Attorney General**	**Rhoda Island Attorney General**	**Massachusetts Attorney General**
Phone	1-410-576-6491	1-877-566-7226 (within North Carolina)	1-401-274-4400	1-617-727-8400

		or 1-919-716-6000 (if outside North Carolina)		
Email	Idtheft@oag.state.md.us	consumer@ncdoj.gov	consumers@riag.ri.gov	AGO@state.ma.us
Address	Identity Theft Unit Attorney General of Maryland 200 St. Paul Place, 16th Floor Baltimore, MD 21202	Consumer Protection Division Attorney General's Office Mail Service Center 9001 Raleigh, NC 27699-9001	Rhode Island Office of the Attorney General 150 South Main Street Providence, RI 02903	Massachusetts AGO One Ashburton Place Boston, MA 02108-1518
Website	https://www.oag.state.md.us/	http://www.ncdoj.gov	http:// www.riag.ri.gov	http://www.mass.gov/ago/

Important notification regarding data breach

Dear [Customer],

New England Biolabs® (NEB®) was recently made aware of a data security incident reported by one of our vendors, who handles web order transactions on www.neb.com. Although we are unaware of any actual misuse of your information, we are providing notice to you and other potentially affected customers about the incident, as well as providing information regarding tools that you can use to protect yourself against possible identity theft or fraud.

What happened?

We were informed on February 13th, 2017 that the e-commerce portion of our website, www.neb.com, experienced an intrusion. Our site is operated for us by a third-party "platform provider", and it was the platform provider's systems that experienced the intrusion. The intruder or intruders placed malware on the platform provider's servers, and, by doing so, gained access to our customers' information, including payment card data, where it existed. To date, the investigation indicates that the intrusion began in February 2016 and ended in December 2016. The attackers gained access to customer information, including payment card numbers, if used, as customers made transactions on the platform provider's systems. The attackers additionally had access to historical customer and payment card data, again, where it existed.

Unfortunately, the platform provider did not discover the breach until November 2016. When they then contacted law enforcement about the breach, law enforcement officials asked that notification to customers be delayed to allow the investigation to move forward.

As you have provided your data and payment information to us in the past, we are now notifying you about this data breach.

What information was involved?

The information that the attacker had access to includes your first and last name, your address, your phone number, and any debit or credit card numbers with expiration dates that you may have used on our website.

What action is being taken?

Our platform provider has worked with a leading cybersecurity firm to remove the malware from its systems and is now actively monitoring the platform to safeguard personal information. Our platform provider has also contacted and offered its cooperation to federal law enforcement.

What You Can Do.

To protect yourself from the possibility of identity theft, if you used a credit or debit card on www.neb.com, we recommend you immediately contact your card company and inform them that your card information may have been compromised, so that they can issue you a

replacement card. Review your banking and card statements and report any suspicious activity to the relevant financial institutions.

For more information on identity theft, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov.

Please be assured that NEB takes matters of data security very seriously. We will continue to work with this platform provider in the ensuing weeks to ensure our online ordering system remains well protected.

We apologize for this inconvenience and thank you for the continued trust you place in NEB. If you have any questions regarding this incident, please contact me at ITinfo@neb.com.

Sharon Kaiser
CIO, Director Information Technology

New England Biolabs, Inc.

[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

Plow & Hearth 7021 Wolftown-Hood Rd., Madison, VA 22727
540.948.2272 www.plowandhearth.com

[Insert date]

[Name]
[Address]
[City], [State] [ZIP]

Dear **[Name]**,

We are writing to notify you of an incident that involves certain of your personal information. The third-party company contracted to operate our e-commerce platform, Aptos, Inc. ("Aptos"), which also supports our brands Wind & Weather, HearthSong, Magic Cabin, and Problem Solvers, and formerly supported our subsidiary's brand Reuseit, informed us on February 6, 2017, that it had experienced a malware intrusion of its systems last year. To date, the investigation indicates that the intrusion on Aptos' systems occurred between February 2016 and December 2016, and included access to certain of our customers' personal information for transactions during that time period, as well as transactions dating back to 2013. The personal information involved in the incident may have included your name, address, phone number and payment card information (including expiration dates and, in limited cases, security codes). Our records indicate that your credit card(s) ending in [xxxx] was impacted.

We have been informed that Aptos is working with a leading cybersecurity firm and has taken steps to secure systems and determine the nature of the incident. Aptos is also working with law enforcement authorities in their investigation. The credit card companies and issuing banks are being contacted for the purposes of identifying unauthorized charges.

Based on the information we have at this time, there is no evidence that any of the information has been misused as a result of this incident. We regret that this incident may affect you. We take our obligation to safeguard personal information very seriously and are alerting you about this incident so you can take steps to help protect yourself. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.

We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports. Furthermore, the attached Reference Guide provides recommendations by the U.S. Federal Trade Commission on the protection of personal information.

We hope this information is useful to you. If you have any questions regarding this incident, please call **1-800-303-0562, Monday through Friday 9:00am to 6:00pm, eastern standard time.**

Again, we regret any inconvenience this may cause you.

Sincerely,

Dana Pappas, CFO

Reference Guide

We encourage our affected customers to take the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office as it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends the following steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information. The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
http://www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

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

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $10 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

[RETURN MAIL ADDRESS – Inserted By AllClear ID]

[First_Name] [Last_Name]
[Address_Line_1]
[Address_Line_2]
[City], [State] [Zip]

[Date]

Dear [First_Name] [Last_Name],

We are writing to inform you of an incident that may have involved your personal information. An incident involving unauthorized access to information associated with certain purchases made on our website vapourbeauty.com. On February 9, 2017, we were notified of the incident by Aptos, the third-party digital platform provider that hosts our ecommerce site. We wanted to share information and inform you that Vapourbeauty.com, Aptos and law enforcement are responding. Although we have not been informed of any actual misuse of your information, we wanted to provide you this notice and information on how you can protect your credit and debit accounts.

You may wonder why you are hearing about the breach now. We understand that Aptos contacted Federal law enforcement agencies and the U.S. Department of Justice at that time. Law enforcement requested that notification to businesses (including Vapourbeauty.com) and customers be delayed to allow the investigation to move forward.

What Information Was Involved?
Aptos has informed us that attackers had access to the following online data associated with orders made before «Date»:

- First and last name,
- Address,
- Phone number,
- Email address, and
- Debit or credit card number with expiration dates.

What Happened?
On February 9, 2017, we were informed that Aptos experienced a security incident last year that involved our website (Vapourbeauty.com). Aptos has indicated that the intrusion began in February 2016 and ended in December 2016. During that time, we understand that cyber criminals placed malware on Aptos' servers and gained access to Vapourbeauty.com's data. We have been assured that the malware has been removed and that the criminals no longer have access to their systems or data.

We want to make you aware of steps you may take to guard against identity theft or fraud. Please review the enclosed Information about Identity Theft Protection.

[REQUIRED PRODUCT/SERVICE LANGUAGE START]

As an added precaution, we have arranged to have AllClear ID protect your identity for «Time» 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 «Time» months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call «DID_Phone» 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. You may sign up online at enroll.allclearid.com or by phone by calling «DID_Phone» using the following redemption code: {RedemptionCode}.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

[REQUIRED PRODUCT/SERVICE LANGUAGE END]

We at Vapourbeauty.com, take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. We have been working with Aptos to learn more about the incident. Aptos has indicated that it has worked with a leading cybersecurity firm to remove the malware from its systems and is actively monitoring the platform to safeguard personal information.

For More Information

We have limited information to share beyond what is provided in this notice and still we understand that you may have additional questions or concerns. Please feel free to reach out to our dedicated hotline at AllClear ID Monday through Saturday, 8 a.m. to 8 p.m. Central Time at 1-855-336-6688 and AllClear ID will work with you to address your questions and concerns

Sincerely,

[Tera Romero, Records]
[Vapour Organic Beauty]
[PO BOX 99 TAOS, NM 87571]