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

Office of the Attorney General
Attn: Computer Data Security Incident
33 Capitol Street
Concord, NH 03301

October 26, 2017

To Whom It May Concern:

Consistent with N.H. Rev. Stat. §§ 359-C:20, this letter provides notice of a data security incident. Alpha Industries, Inc. ("Alpha") is a clothing manufacturer and apparel retailer that is engaged in online business with individual customers residing in New Hampshire through its website www.alphaindustries.com. Alpha utilizes a digital commerce platform on its website provided by third-party Aptos, Inc. ("Aptos"). As a result, Aptos holds the data of individual customers associated with their transactions on Alpha websites.

Alpha sent a prior notice to your office regarding this incident on October 2, 2017. This letter supplements that earlier notice with additional information recently provided by Aptos.

On August 25, 2017, Aptos notified Alpha that Aptos had experienced an intrusion whereby the intruder(s) accessed Aptos' digital commerce platform and may have acquired certain personal information of customers who manually entered their payment card details on Alpha's website and the websites of other retailers. No data was provided at that time regarding which customers were affected. The intrusion apparently began on July 6, 2017 and ended on August 9, 2017. The personal information that the intruder(s) may have had access to includes customers' first and last names, addresses, email addresses, and debit or credit card numbers with expiration dates and CVV verification codes.

Aptos first provided information on which of Alpha's customers were potentially affected by the breach on September 8. That data indicated that a total of 634 Alpha customers overall were potentially affected by the intrusion, including one with a billing address in your state. On September 26, Aptos provided Alpha reorganized data regarding potentially affected customers in response to questions from Alpha. On October 17, Aptos formally provided notice that additional Alpha customers were affected by the incident. The same day, Aptos provided updated data regarding potentially affected customers to supplement data Aptos sent on September 8. The updated data indicates that additional Alpha customers may have been affected by the incident.

On approximately October 2, 2017, Alpha provided notice to its affected U.S. customers, including those with a billing address in your state, who were listed in the data Aptos provided on September 8. Alpha also timely notified relevant state agencies.

The October 17 spreadsheet indicates that a total of approximately 1,500 Alpha customers were potentially affected by the incident, including 909 who were not listed in the September 8 data. Of those 909, six have billing addresses in your state.

We understand that Aptos has engaged a leading cybersecurity firm to determine the scope of the matter and has been working to improve the security of its e-commerce solution. As part of that effort, we understand that Aptos removed the malicious code and disabled the page used to gain access to its system. Aptos reports that it has since filtered the code to remove non-alphanumeric characters and has created an alert that is designed to highlight attempts to modify the code. Aptos has also contacted and offered its cooperation with federal law enforcement, specifically the Federal Bureau of Investigation.

Alpha will be providing written notice to the six customers with billing addresses in New Hampshire, who were not previously notified of the incident because they were not listed in the September 8 data, along with additional affected customers in other states, on approximately Monday, October 30. A form copy of the notice that will be sent to the affected New Hampshire customers is included as Exhibit A.

In addition, Alpha is offering, for one year, complimentary credit monitoring and an identity theft restoration product by TransUnion, managed by Epiq Systems, to help alleviate any concerns affected customers may have. Alpha has also established a call center to provide information to affected customers.

Alpha is committed to full cooperation in answering any questions that your office may have.

Respectfully yours,

Michael Cirker
CEO

Francis Conduah
Controller

# Exhibit A

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

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

**Notice of Data Breach**

Dear <<Name1>>:

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 August 25, 2017, that our website www.alphaindustries.com was involved in a security incident. Our website is operated for us by a third-party platform provider, Aptos, and it was Aptos that experienced the intrusion. Aptos first provided information on which of our customers were potentially affected by the breach on September 8. On September 26, Aptos provided Alpha reorganized data regarding potentially affected customers in response to questions from Alpha. On October 17, Aptos formally provided notice that additional Alpha customers were affected by the incident. The same day, Aptos provided updated data regarding potentially affected customers to supplement data Aptos sent on September 8. The updated data indicates that additional Alpha customers may have been affected by the incident.

To date, the investigation indicates that the intrusion began on approximately July 6, 2017 and ended on August 9, 2017. The intruder(s) accessed Aptos' e-commerce solution, used to facilitate online purchases on our website, and may have acquired certain personal information of our customers who manually entered their payment card details on our website during the intrusion period (July 6 to August 9, 2017).

We are notifying you because your information appeared in the data provided to us by Aptos regarding which of our customers were potentially affected by the breach.

**What Information Was Involved?**

The personal information that the intruder(s) had access to includes your first and last name, your address, your email address, and any debit or credit card numbers with expiration dates and CVV verification codes that you manually entered on our website. To date, we believe that no social security numbers or passwords were accessed.

**What Are We Doing?**

We understand that Aptos has engaged a leading cybersecurity firm to determine the scope of the matter and has been working to improve the security of its e-commerce solution. As part of that effort, we understand that Aptos removed the malicious code and disabled the page used to gain access to its system. Aptos reports that it has since filtered the code to remove non-alphanumeric characters and has created an alert that is designed to highlight attempts to modify the code. Aptos has also contacted and offered its cooperation to federal law enforcement, specifically the Federal Bureau of Investigation. In addition, we are offering complimentary credit monitoring and an identity theft restoration product by TransUnion, and managed by Epiq Systems, 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.

**What Services Are We Offering?**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or off line credit monitoring service anytime between now and January 31, 2018. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new

public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and identity theft insurance.

**For More Information**

We at Alpha 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

888-396-9530, 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,

Michael Cirker
CEO

Francis Conduah
Controller