Alyssa Watzman, Partner
1801 Broadway, Suite 529
Denver, Colorado 80202
awatzman@constangy.com

March 29, 2023

VIA ELECTRONIC MAIL

Attorney General Raul R. Labrador
Office of the Attorney General
Consumer Protection Division
700 W. Jefferson Street
P.O. Box 83720
Boise, ID 832720-0010

Re: Notice of Data Security Incident

Dear Attorney General Labrador:

Constangy, Brooks, Smith and Prophete LLP ("Constangy") represents Svanaco, Inc. d/b/a AmericanEagle.com (the "Company") in connection with a data security incident described in greater detail below. The Company is a web design, development, and digital marketing agency headquartered in Des Plaines, Illinois that builds and hosts e-commerce platforms.

1. **Nature of Incident**

On November 16, 2022, the Company was alerted to unusual activity involving an e-commerce platform belonging to one of its customers. Upon learning of this activity, the Company took immediate steps to further secure the e-commerce platform and associated payment card information. The Company also promptly engaged a nationally recognized digital forensics and incident response firm to conduct an independent forensic investigation to determine what happened and whether payment card information had been accessed or acquired without authorization. As a result of that investigation, on March 1, 2023, the Company received confirmation that information associated with payment cards processed through e-commerce platforms belonging to www.leonisa.com appeared to have been accessed or acquired without authorization between July 13, 2022 and December 9, 2022. The Company then worked diligently to identify all potentially affected individuals and to coordinate with relevant customers for purposes of notification.

The personal information potentially accessed or acquired by a malicious actor in connection with this incident includes names, payment card numbers, payment card expiration dates, and payment card security codes.

2. **Number of Idaho residents affected**

The Company notified twenty-seven (27) Idaho residents of the incident via first class U.S. mail on March 29, 2023. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the incident

As soon as the Company learned of this incident, the Company took steps to secure impacted e-commerce platforms and associated payment card information. In addition, the Company engaged a leading, independent digital forensics and incident response firm to conduct a forensic investigation. The Company also reported the incident to various payment card brands as well as law enforcement to help protect potentially impacted information and prevent fraudulent activity. Further, in order to reduce the likelihood of a similar incident occurring in the future, the Company has implemented measures to enhance the security of all e-commerce platforms hosted on behalf of its customers.

4. Contact information

The Company takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at (720) 292-2052 or AWatzman@constangy.com.

Sincerely yours,

Alyssa R. Watzman of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Encl.: Sample Consumer Notification Letter

P.O. Box 989728
West Sacramento, CA 95798-9728

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

March 29, 2023

Re: Notice of Data <<Breach or Security Incident>>

Dear <<FIRST NAME>> <<LAST NAME>>:

Svanaco, Inc. d/b/a Americaneagle.com ("Americaneagle.com") is writing to notify you of a data security incident relating to a purchase you made at https://www.leonisa.com, which may have involved your payment card information.[1] Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

Who is Americaneagle.com? Svanaco, Inc. d/b/a Americaneagle.com ("Americaneagle.com") is a web design, development, and digital marketing agency that builds and hosts websites and e-commerce platforms for other businesses, including https://www.leonisa.com. Americaneagle.com does not sell any products directly to consumers; instead, Americaneagle.com develops web platforms that allows consumers to purchase products from their favorite brands. Americaneagle.com is ***not*** the clothing company you may be familiar with.

What Happened? On November 16, 2022, Americaneagle.com was alerted to unusual activity involving the online store it hosts for https://www.leonisa.com. Upon learning of this activity, Americaneagle.com took immediate steps to secure the online store and associated customer information. Americaneagle.com also promptly engaged a nationally-recognized digital forensics and incident response firm to conduct an independent forensic investigation to determine what happened and whether customer payment card information was involved. As a result of that investigation, on March 1, 2023, Americaneagle.com learned that payment card information processed through https://www.leonisa.com between August 17, 2022 and December 7, 2022 may have been accessed or acquired without authorization. **The unusual activity occurred exclusively on the Americaneagle.com web platform. Leonisa did *not* experience a data security incident.**

What Information was Involved? The potentially impacted payment card information includes names, payment card numbers, expiration dates, and security codes.

What Are We Doing? As soon as Americaneagle.com discovered this incident, Americaneagle.com took the steps described above. In addition, Americaneagle.com reported the incident to the various payment card brands as well as law enforcement in an effort to protect potentially impacted information and prevent fraudulent activity. Further, in order to reduce the likelihood of a similar incident occurring in the future, Americaneagle.com has implemented measures to enhance the security of all hosted e-commerce platforms. Americaneagle.com is also providing you with information about steps that you can take to help protect your personal information.

[1]Americaneagle.com is a web design, development, and digital marketing agency that built and hosts the e-commerce platform belonging to Leonisa, from which you made a credit / debit card purchase.

What You Can Do: You can follow the recommendations provided on the following page to help protect your personal information. Americaneagle.com also recommends that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call IDX at (833) 753-4471 from 8:00 A.M. to 8:00 P.M. Central Time, Monday through Friday (excluding holidays). IDX call center representatives are fully versed on this incident and can answer any questions that you may have.

Please accept my sincere apologies and know that Americaneagle.com takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Mike Svanascini, CEO
Svanaco, Inc d/b/a Americaneagle.com

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

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).

Request a Copy of Your 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 https://www.annualcreditreport.com, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Place a 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 one year. 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 https://www.annualcreditreport.com.

Put a Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. 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. 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: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission (FTC)
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.