MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Vincent F. Regan
Office: (267) 930-4842
Fax: (267) 930-4771
Email: vregan@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

November 30, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Etz Hayim Holdings, SPC. d/b/a Lazarus Naturals ("Lazarus Naturals") located at 1116 Northwest 51st Street Seattle, WA 98107, and are writing to notify your office of an incident that may affect the security of some personal information relating to seventy (70) New Hampshire residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Lazarus Naturals does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 14, 2020, Lazarus Naturals identified suspicious activity on its website. Lazarus Naturals immediately began an investigation, with the assistance of third-party forensic specialists, to assess the nature and scope of the incident. Through an investigation, it was determined that malicious code was inserted by an unauthorized individual on the checkout page of its website from September 5, 2020 to September 14, 2020 which may have had the ability to capture customer information while making a purchase. The information that could have been subject to unauthorized access includes name, address and payment card information (account number, card expiration date and security code).

Notice to New Hampshire Residents

On or about November 30, 2020, Lazarus Naturals provided written notice of this incident to all affected individuals, which includes seventy (70) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Lazarus Naturals moved quickly to investigate and respond to the incident, assess the security of its systems, and notify potentially affected individuals. Lazarus Naturals also implemented additional safeguards and training to its employees. Lazarus Naturals is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for one (1) year through TransUnion at no cost to the individuals.

Additionally, Lazarus Naturals is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Lazarus Naturals is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Lazarus Naturals is reporting this matter to regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4842.

Very truly yours,

Vincent F. Regan of
MULLEN COUGHLIN LLC

VFR/pls
Enclosure

EXHIBIT A

Lazarus Naturals

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>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Breach

Dear <<Name 1>>,

We are writing to inform you of an incident we discovered regarding our website that may affect the security of some of your personal information. Between September 5 and September 14 we experienced a malicious attack, during which our customers' information may have been captured. You are receiving this notice because you made a purchase on the website during this timeframe and your payment card information may be at risk.

What We Are Doing. We are extremely sorry for any inconvenience or harm that this incident may have caused you and are committed to earning back your trust. The security of your credit card information and privacy of interactions is of upmost importance to us at Lazarus Naturals. We have taken exhaustive steps to ensure that your information and privacy will be protected in the future and do not take this situation lightly. Since the incident was discovered we have taken the following steps to secure your information:

- Immediately removed the malicious code and conducted a thorough internal investigation of what happened, how it happened, and how to prevent it in the future
- Engaged a third-party forensic investigation team to review our internal processes, systems, and other relevant information, who confirmed we took the proper steps to protect our customers.
- Enacted new security protocols and restructured our server architecture to remove the possibility of a similar situation in the future.
- Notified potentially impacted customers of the incident via this letter with ways you can protect your personal information.

At the same time we were conducting our investigation, we implemented a planned migration from our previous website platform on which this incident occurred, to a new, more secure, platform. We do not expect to experience a similar issue on our new website.

What Happened? On September 14, 2020, we identified suspicious activity on our website and immediately began an investigation with the assistance of third-party forensic specialists to assess the nature and scope of the incident. Through the investigation, it was determined that malicious code was inserted by an unauthorized party on the checkout page of our website from September 5, 2020 to September 14, 2020 which may have had the ability to capture customer information while making a purchase.

What Information Was Involved? Our investigation determined the type of information potentially impacted by this incident includes your name, address, and payment card information (account number, card expiration date and security code). We do not store any payment information after purchase so only information entered between September 5, 2020 and September 14, 2020 may have been impacted.

What Can You Do? We have arranged to have TransUnion provide credit monitoring and identity protection services to you for one (1) year at no cost to you as an added precaution. Please review the enclosed *Steps You Can Take to Help Protect Your Information* for instructions on how to enroll in these services.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-914-4709 (toll free), Monday through Friday from 6:00 am to 6:00 pm Pacific Time.

I take this matter to heart and am committed to ensuring nothing of this sort ever happens again.

Sincerely,

Sequoia Price-Lazarus
Founder and CEO
Etz Hayim Holdings, SPC. d/b/a Lazarus Naturals

Steps You Can Take to Help Protect Help Against Identity Theft and Fraud

Activate Identity Monitoring

How to Enroll: You can sign up online or via U.S. mail delivery

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 12-letter Activation Code **<<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 six-digit telephone passcode **<<6-digit 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 offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. 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.

Monitor Your Accounts

The confidentiality, privacy and security of your personal information is one of our highest priorities. That is why we are sharing these steps you may take to protect your identity and uncover any fraudulent activity on your accounts.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly, as set forth below, to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either the police report, investigative report or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

You may further educate yourself regarding identity theft, fraud alerts, security freezes and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission or your state Attorney General.

The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover their information has been misused to file a complaint with them. You may obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note in order to file a report with law enforcement for identity theft, you likely will need to provide some proof that you have been a victim. Instances of known or suspected identity theft should be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Maryland residents, the Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 53 Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; https://oag.dc.gov.