

Via Email

August 2, 2023

Email: IDTheft@oag.state.md.us

Attorney General Anthony G. Brown
MD Office of Attorney General
200 St. Paul Place
Baltimore, MD 2120

Re: Lazarus Naturals' Data Incident Notification

Dear Attorney General Anthony Brown:

On behalf of our client, Etz Hayim Holdings, S.P.C. dba Lazarus Naturals ("Lazarus Naturals"),¹ we are writing to provide information regarding a security incident involving customer personal information (the "Incident").²

On July 10, 2023, Lazarus Naturals discovered that customer personal information was likely accessible to an unauthorized actor(s) as a result of the Incident. The Incident was caused by one or more malicious actors who exploited a software vulnerability on Lazarus Naturals' website allowing them to insert malicious code facilitating the compromise. Based on the investigation, it appears the Incident occurred at Lazarus Naturals at certain points between March 1 and June 2, 2023.

Upon learning of the Incident, Lazarus Naturals launched an in-depth investigation to determine the scope of the Incident and identify those potentially affected. This included working with its information technology team and engaging third-party forensic experts in an effort to ensure the Incident did not result in any additional exposure to personal information and taking steps to confirm the integrity of Lazarus Naturals' systems. We also worked with third-party experts to determine what information may have been at risk.

Lazarus Naturals has determined at this point in its investigation that personal information relating to its customers may have been disclosed to the unauthorized actor(s) as a result of the Incident. The personal information may have included full name, billing address, and financial information (such as credit or debit card information including card number, expiration date and printed card security code). However, registered users using stored payment and delivery information may not have had their information accessed. Based on our investigation to date, we do not believe Social Security numbers, dates of birth, or driver license numbers were involved in this Incident.

¹ Lazarus Naturals' corporate address is: 16427 NE Airport Way, Portland, OR 97230.

² Please note that by providing this letter Lazarus Naturals is not agreeing to the jurisdiction of Maryland, or waiving its right to challenge jurisdiction in any subsequent actions. We are providing this notification as a courtesy.

To date, Lazarus Naturals has identified 42,000 individuals whose personal information may have been impacted by the Incident, of which 689 are believed to be Maryland residents.

Lazarus Naturals has been in contact with law enforcement, including the Federal Bureau of Investigation ("FBI"), and is supporting law enforcement's investigation.

On August 3, 2023, Lazarus Naturals commenced the notification process and begun mailing notices to affected individuals. Enclosed is the specimen letter being provided to affected individuals so they can take steps to minimize the risk that their information will be misused. Lazarus Naturals will also be making credit monitoring and ID restoration protection services available at no cost to potentially affected persons. For persons who timely enroll, these services will be available for 24 months.

Lazarus Naturals has taken numerous steps to protect the security of the personal information of the affected individuals. To help ensure an incident like this will not occur in the future, Lazarus Naturals is reviewing its policies and procedures to make sure employees are reminded about best practices on data security.

If you require any additional information on this matter, please do not hesitate to contact me.

Very truly yours,

JACKSON LEWIS P.C.

Joseph J. Lazzarotti

Joseph J. Lazzarotti

Encl.



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

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

August 3, 2023

Re: <<Variable Data 2>>

Dear <<Name 1>>:

At Etz Hayim Holdings, S.P.C. d/b/a Lazarus Naturals ("Lazarus Naturals") we value and respect the privacy of your information, which is why we are writing to inform you we recently learned that some of your personal information may have been subject to unauthorized access or acquisition as the result of a cyberattack (the "Incident"). While we are not aware of any misuse of your information, we are providing this notice to inform you of the Incident and to call your attention to steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened?

On July 10, 2023, Lazarus Naturals discovered your personal information was likely accessible to an unauthorized actor(s) as a result of the Incident. The Incident was caused by one or more malicious actors who exploited a software vulnerability on our website allowing them to insert malicious code facilitating the compromise. Based on the investigation, it appears the Incident occurred at Lazarus Naturals at certain points between March 1 and June 2, 2023.

What Information Was Involved?

The following types of data may have involved in this incident: personal information such as your name and billing address; and financial information such as credit or debit card information including card number, expiration date and printed card security code. However, if you checked out as a registered user using stored payment and delivery information, that information may not have been accessed. Based on our investigation to date, we do not believe Social Security numbers, dates of birth, or driver license numbers were included in the breach.

What We Are Doing.

Lazarus Naturals takes this Incident and the security of your personal information very seriously. Upon learning of this incident, we launched an in-depth investigation to determine the scope of the Incident and identify those potentially affected. This included working with our information technology team and engaging third-party forensic experts in an effort to ensure the Incident did not result in any additional exposure to personal information and taking steps to confirm the integrity of Lazarus Naturals' systems. We also worked with third-party experts to determine what information may have been at risk. Lazarus Naturals has also reported the Incident to the Federal Bureau of Investigation ("FBI") to assist in our investigations and best protect from any incidents like this in the future. This communication was not delayed at the request of law enforcement. As an added precaution, we are also offering complimentary access to identity monitoring, fraud consultation, and identity theft restoration services. If you wish to receive these services, activation instructions are below.

What You Can Do.

The attached sheet describes steps you can take to protect your identity and personal information. To help protect your identity, we are offering complimentary access to **Equifax Credit Watch - Gold** for **24 months**. Key features of this offering include:

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft

To activate your membership and start monitoring your personal information, please ensure that you enroll by following the Enrollment Instructions on the attached Equifax document, no later than **October 31st, 2023**.

For the sake of convenience, the enrollment instructions for **Equifax Credit Watch - Gold** for **24 months** may also be referenced here:

Go to www.equifax.com/activate

Enter your unique Activation code included on the attached Equifax document, then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

For More Information.

Lazarus Naturals apologizes for the inconvenience this may cause. We are committed to maintaining the security and privacy of personal information. We want you to be assured that we are taking steps to minimize the chances of a similar occurrence happening again. We understand that 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 833-627-2752, Monday through Friday from Monday through Friday from 6:00 a.m. to 6:00 p.m. PT, excluding holidays.

Regards,

A handwritten signature in black ink, appearing to read 'D. Summers', with a stylized flourish at the end.

Dylan C. Summers
Chief Revenue Officer
Etz Hayim Holdings, S.P.C. d/b/a Lazarus Naturals

ADDITIONAL RECOMMENDED STEPS

We recommend you remain vigilant and consider taking the following steps to avoid identity theft, obtain additional information, and protect your personal information:

- Order Your Free Credit Report at www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information.
- Place a Fraud Alert on Your Credit File. A fraud alert helps protect you against an identity thief opening new credit in your name. With this alert, when a merchant checks your credit history when you apply for credit, the merchant will receive a notice that you may be a victim of identity theft and to take steps to verify your identity. You also have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can place a fraud alert or request a security freeze by contacting the credit bureaus. The credit bureaus may require that you provide proper identification prior to honoring your request.

Equifax	P.O. Box 740241 Atlanta, GA 30374	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 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
- If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
- The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission ("FTC"). You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.
- *For District of Columbia Residents:* You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov.

- *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.
- *For New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to <http://consumersunion.org/pdf/security/securityNM.pdf>
- *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov/internet/resource-center>; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or <https://dos.ny.gov/consumer-protection>.
- *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.
- *For Rhode Island Residents:* You can obtain information from the Rhode Island Attorney General about steps you can take to help prevent identity theft at: 150 South Main Street, Providence, RI 02903, (401) 2744400, www.riag.ri.gov. [REDACTED]



<<Name 1>>

Enter your Activation Code: <<ACTIVATION CODE>>

Enrollment Deadline: October 31st, 2023

Equifax Credit Watch[™] Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<ACTIVATION CODE>> then click “Submit” and follow these 4 steps:

5. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

6. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

7. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

8. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. ²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer

Services LLC. ³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com ⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. \