Michael Best & Friedrich LLP
Attorneys at Law
Linda C. Emery, CIPP/US
T 414.225.2777
E lcemery@michaelbest.com

January 6, 2025

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: Idtheft@oag.state.md.us

RE: Notice of Data Security Incident

Dear Attorney General Brown:

We represent Blue Diamond Herbs LLC ("Blue Diamond"), located at 8201 Arrowridge Boulevard, Suite 147, Charlotte, NC 28273. We are writing to notify your office of a data security incident Blue Diamond recently experienced, which may have impacted the personal information of two (2) Maryland residents. We will supplement this notice if Blue Diamond learns of any new material information. By providing this notice, Blue Diamond does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data security incident notification statute, or personal jurisdiction. In this letter, we explain what happened, the steps Blue Diamond has taken to address the situation, and how Blue Diamond is providing support to impacted individuals.

Nature of the Data Security Incident

On September 29, 2024, Blue Diamond began to investigate some suspicious activity on its website. As soon as Blue Diamond identified the suspicious activity, it began immediately working with IT cybersecurity experts to assist in investigating the situation.

On November 22, 2024, Blue Diamond confirmed that a bad actor had embedded malicious software code within its website and it temporarily suspended the acceptance of credit cards from its website. This malicious code was used to intercept customer credit card data. Blue Diamond removed the malicious code from the website and launched an updated website with enhanced security features.

Blue Diamond determined that the following personal information of Maryland residents may have been impacted: the individual's name, home address, and credit card number.

Notice to Maryland Residents

On January 7, 2025, Blue Diamond will provide written notification via U.S. Mail to the two (2) Maryland residents impacted by the data security incident. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit A**.

What Blue Diamond is Doing

Blue Diamond consulted with external cybersecurity experts to investigate and respond to this matter. Blue Diamond temporarily stopped accepting online credit card payments to mitigate any risks of additional unauthorized access. In December, Blue Diamond launched a new website with enhanced security features for processing payments.

Blue Diamond secured the services of Kroll to provide identity monitoring at no cost to impacted individuals for 12 months. The offered identity monitoring services include credit monitoring, fraud consultation, and identity theft restoration. Blue Diamond has also created a call center for impacted individuals in order to assist people with enrolling in the credit and identity monitoring services and answer questions regarding the data security incident.

Contact Information

Blue Diamond remains dedicated to protecting the personal information it maintains. If you have any questions or would like any additional information, please do not hesitate to contact me by phone or email:
Phone: (414) 225-2777
Email: lcemery@michaelbest.com

Sincerely,

Michael Best & Friedrich, LLC

Linda C. Emery

Linda C. Emery

Enclosure: Individual Notification Letter

EXHIBIT A

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: **Notice of Data Breach**

Dear Valued Customer:

Blue Diamond Herbs LLC ("Blue Diamond") values the privacy of our customers. We are writing to notify you about a cybersecurity incident we recently experienced, which may have impacted your personal information. In this letter, we explain what happened, the steps we have taken to address the situation, and how we are providing you support in light of the cybersecurity incident. We have also outlined additional steps you may take to help protect yourself against potential misuse of your personal information.

What Happened

On September 29, 2024, we began to investigate some suspicious activity on our website. As soon as we identified the suspicious activity, we began immediately working with IT cybersecurity experts to assist in investigating the situation.

On November 22, 2024, we confirmed that a bad actor had embedded malicious software code within our website and we temporarily suspended the acceptance of credit cards from our website. This malicious code was used to intercept customer credit card data. We have removed the malicious code from our website and the website has returned to normal operation.

Based on our findings from the investigation of the cybersecurity incident, we have determined that some of your personal information was impacted by the cybersecurity incident. We deeply regret that this cybersecurity incident occurred and that it impacted your personal information.

What Information Was Involved

The personal information involved includes: first and last name, home address, and credit card number.

What We Are Doing

We consulted with external cybersecurity experts to investigate and respond to this matter. We temporarily stopped accepting online credit card payments to mitigate any risks of additional unauthorized access. In December, we launched a new website with enhanced security features for processing payments.

We have also secured the services of Kroll to provide you with free identity monitoring for <<Monitoring Term Length (Months)>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people whose personal information has been impacted by a data security incident. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until ***<<b2b_text_6(activation deadline)>>*** *to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

What You Can Do

Please review the enclosed "Additional Information on Credit Monitoring & Identity Theft" section included with this letter. This section describes additional steps you can take to help protect yourself from identity theft. We recommend that you remain vigilant about protecting and monitoring your financial accounts, credit card statements and credit reports for any suspicious activity. Report suspicious activity to your financial institution, credit card company or credit reporting agency immediately. If you believe that you have been a victim of identity theft, contact your local law enforcement, your state attorney general and the Federal Trade Commission ("FTC").

We trust that the services we are offering to you demonstrate our continued commitment to your security.

For More Information

If you have any further questions or concerns regarding this matter, please contact 1-866-676-3378, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Our customers are the most important part of our business, and we sincerely apologize for any concern this may have caused you. We are redoubling our efforts to strengthen our security to help protect your data.

Sincerely,

Luke DiDio
Owner, Blue Diamond Herbs

Included: Additional Information on Credit Monitoring & Identity Theft

ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT

Please remain vigilant for incidents of fraud and identity theft by reviewing your bank account statements, monitoring free credit reports, and promptly reporting any fraudulent activity or suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

- You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), https://consumer.ftc.gov/features/identity-theft
- You have certain rights under the **Fair Credit Reporting Act** related to your consumer credit. For more information, please go to: https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.
- **Take Charge: Fighting Back Against Identity Theft:** We recommend reviewing the FTC's comprehensive guide on how to guard against and deal with identity theft, available at https://www.identitytheft.gov/.

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 www.annualcreditreport.com, calling 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 can print a copy of the request form at www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies is as follows.

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

For Arizona, Colorado, Florida, Illinois, Indiana, Iowa, Kansas, Massachusetts, Missouri, Nebraska, New Jersey, New York, Ohio, Oregon, Pennsylvania, Tennessee, Vermont, and Wisconsin residents: You may obtain one or more (depending on the state) additional copies of your credit report every 12 months, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. You may want to place a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for 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. You can also have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentation. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies using the contact information above.

Security Freeze. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts under your name. To place a security freeze on your credit report, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, Social Security number, and other personal information.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

- **For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, 1-888-743-0023.
- **For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.
- **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 Connecticut residents:** You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.
- **For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261. https://www.consumerfinance.gov/consumer-tools/credit-reports-and-scores/
- **For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.
- **For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft.
- **For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.