SMITH, ANDERSON, BLOUNT,
DORSETT, MITCHELL & JERNIGAN, L.L.P.

LAWYERS

OFFICES
Wells Fargo Capitol Center
150 Fayetteville Street, Suite 2300
Raleigh, North Carolina 27601

MAILING ADDRESS
P.O. Box 2611
Raleigh, North Carolina
27602-2611

TELEPHONE: (919) 821-1220
FACSIMILE: (919) 821-6800

June 28, 2023

***Via First Class Mail and Electronic Mail to:***

New Hampshire Attorney General
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: attorneygeneral@doj.nh.gov

Re: Data Security Incident Notification Supplement

To whom it may concern:

Our firm represents Pepsi Bottling Ventures LLC ("PBV"), located at 4141 Parklake Avenue, Suite 600, Raleigh, NC 27612-2380. On behalf of PBV, we are writing to update your office of a data security incident described in greater detail below, pursuant to N.H. RSA § 359-C:20(I)(b). We previously notified your office of this same incident by letter dated February 10, 2023.

**A. Nature of the Data Event**

On January 10, 2023, PBV discovered that its systems had been accessed by an outside third-party actor. In response, PBV began an investigation to determine the nature and scope of the activity. The investigation confirmed that PBV's network was subject to unauthorized access on December 23, 2022, until approximately January 19, 2023, when a third-party actor accessed the PBV's systems through malware, and that certain files were downloaded from the PBV's system. In response, PBV worked diligently to secure its systems and determine the nature of the information that may have been impacted, and to whom that information pertained. PBV's investigation has now concluded.

**B. Type of Information and Notice to New Hampshire Residents**

PBV's initial investigation determined that the incident involved personal information for approximately 5 New Hampshire residents. As we stated in our initial report to your office, those previously identified individuals were notified via letter dated February 10, 2023. After conducting a further investigation, PBV determined that the incident involved personal information for approximately 2 additional New Hampshire residents. These additional affected individuals will be sent a letter on or about Wednesday, June 28, 2023 provided in substantially the same form as the letter attached here as **Exhibit A.**

**C. Other Steps Taken and to be Taken**

Upon discovering the incident, PBV moved quickly to contain the incident, investigate, and respond. PBV also assessed the security of its systems, required all employees to change their passwords on accounts associated with PBV, and PBV will take additional steps to reduce the risk of a similar incident occurring in the future, including assessing the implementation of additional technical safeguards. PBV will cooperate with any investigation by law enforcement.

PBV is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including enrolling in complementary identity monitoring services offered in the notification letter. PBV is also advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. PBV is providing individuals with information on how to review and place a fraud alert on their individual credit files, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, and a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports. Additionally, PBV is encouraging affected individuals to contact the Federal Trade Commission, and the appropriate State Attorney General, to report attempted or actual identity theft and fraud.

**D. Contact Information**

This notice may be supplemented, if necessary, with any new significant facts discovered after its submission. By providing this notice, PBV 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.

PBV is dedicated to protecting the sensitive information within its control. Should you have any questions regarding this notification or other aspects of the data security event, please feel free to contact us.

Sincerely,

Jackson Wyatt Moore, Jr.

Enclosure: Form of Notification Letter

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

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

## NOTICE OF SECURITY INCIDENT

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Pepsi Bottling Ventures values our relationship with you, and we respect the privacy of your information. This is why, as a precautionary measure, we are writing to make you aware of an incident that may affect the security of some of your personal information. At this time we are not aware of any identity theft or fraud involving your personal information, but out of an abundance of caution, we are providing you with an overview of the incident, our ongoing response, and resources available to you right now to help protect yourself from any potential consequences.

### WHAT HAPPENED?

On January 10, 2023, Pepsi Bottling Ventures learned that unauthorized activity was reported on certain of our internal IT systems. Based on our preliminary investigation, an unknown party accessed those systems on or around December 23, 2022, installed malware, and downloaded certain information contained on the accessed IT systems.

We took prompt action to contain the incident and secure our systems. While we are continuing to monitor our systems for unauthorized activity, the last known date of unauthorized IT system access was January 19, 2023. We reported the incident to law enforcement and are cooperating with their investigation.

### WHAT INFORMATION WAS INVOLVED?

### WHAT WE ARE DOING

Pepsi Bottling Ventures LLC values your privacy and deeply regrets that this incident occurred. Pepsi Bottling Ventures LLC is conducting a thorough review of the potentially affected records and systems. The safety of your personal information is of the utmost importance to us. Pepsi Bottling Ventures promptly reported the incident to law enforcement, suspended all affected systems, and began an investigation to understand the scope and impact of the incident. We have taken a number of steps to contain the unauthorized access, further strengthen the security of our networks, and increase technological security by requiring the change of all company passwords.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for . Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visi 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 promptly change your username(s), password(s), and security question answer(s) for any accounts or account information you maintain with Pepsi Bottling Ventures, and take any other appropriate steps to protect all other online accounts maintained by you that use the same username, password, or security question answer.

Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information, and how to receive free identity monitoring services for one year.

**FOR MORE INFORMATION**

For further information and assistance, please contact , Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

Derek Hill
President & CEO
4141 Parklane Ave, Suite 600
Raleigh, NC 27612

KROLL

## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

**Triple Bureau Credit Monitoring and Single Bureau Credit Report**

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will 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.

**Web Watcher**

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

**Public Persona**

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

**Quick Cash Scan**

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

**$1 Million Identity Fraud Loss Reimbursement**

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

**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.

## Steps You Can Take to Further 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 for fraud or identity theft. 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, including your state attorney general and the Federal Trade Commission (FTC). You should change passwords and security questions on affected accounts.

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 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 access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or you can elect to 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 for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

We recommend placing a fraud alert on your credit report. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Additional information is available at http://www.annualcreditreport.com.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

**OTHER IMPORTANT INFORMATION**

- **Security Freeze**

A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency.

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. There is no charge to request a security freeze or to remove a security freeze.

- **Additional information required by certain State laws**

**Maryland** residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

**New Mexico** Consumers have the right to obtain a Security Freeze or Submit a Declaration of Removal. A summary of your rights under the Fair Credit Reporting Act can be found at https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.docx

The **New York** 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/.

**North Carolina** residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/ or at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 877-566-7226 (Toll-free within North Carolina), 919-716-6000

The **Oregon** Attorney General may be contacted to report suspected identity theft at:doj.state.or.us/ or the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, in addition to local law enforcement and the FTC.

**Wisconsin** Residents: upon Pepsi Bottling Ventures' receipt of a written request from an affected person receiving this notice, we will identify that person's specific personal information that may have been acquired.

For **Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont** Residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).