Cooley

Randy V. Sabett
+1 202 728 7090
rsabett@cooley.com

By Certified Mail Return Receipt Requested

December 14, 2018

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

Re: Legal Notice of Data Incident

Dear Sirs or Madams:

I write on behalf of my client, Beverages & More, Inc. ("BevMo"), to inform you of a data incident involving the personal information of certain BevMo customers, including three (3) New Hampshire residents. BevMo is notifying these individuals and outlining some steps they may take to help protect themselves.

BevMo was recently notified of a potential data incident by NCR Corporation ("NCR"), the company that operates and maintains BevMo's ecommerce platform at www.bevmo.com. According to the information that BevMo received from this vendor on November 19, 2018, an unauthorized individual was able to gain access to the BevMo website and insert a malicious script designed to capture payment card information entered into the BevMo checkout page. Specifically, the malicious script may have affected the following types of information entered on the BevMo website between August 2, 2018 and September 26, 2018: name, credit or debit card number, expiration date, CVV2 code, billing address, shipping address and phone number.

BevMo takes the privacy of personal information seriously. According to the information BevMo received from NCR, the vendor promptly removed the malicious code after discovering the script and engaged an outside forensic investigation firm to assist with investigating and remediating this incident. BevMo also engaged separate independent forensic experts to assist with the company's own investigation of this matter and is working diligently with the investigators and with NCR. To help prevent something like this from happening again in the future, NCR is continuing to enhance security controls and monitor its systems to further detect and prevent unauthorized access. In addition, BevMo has been in contact with law enforcement and the payment card companies about this incident and will continue to cooperate in the investigations.

Affected individuals are being notified via written letter with information about the incident, the types of information affected, and contact information where individuals may obtain additional information. These notifications have been provided to a notification vendor and will begin mailing the week of December 17-21, 2018. A form copy of this notice is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at +1 (202) 728-7090 or rsabett@cooley.com.

Cooley

Best regards,

Randy V. Sabett

RVS:ELL

Enclosure

193988165 v1

Beverages & More, Inc.

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name1>>:

Notice of Data Incident

BevMo recently learned of a data incident from the ecommerce service provider that operates our website at www.bevmo.com. This incident may have affected certain customers' payment card numbers and other information entered on the BevMo website for a limited period of time. We are providing this notice as a precaution to inform potentially affected customers about this incident and to call your attention to steps you can take to help protect your personal information. We sincerely regret any concern this may cause you.

What Happened

Based upon information that we have received to date from the service provider that operates our website (NCR Corporation) and the results of a third party forensic investigation sponsored by NCR, we believe that an unauthorized individual was able to gain access to the BevMo website and install malicious code on our checkout page. This code was designed to capture payment information and may have affected certain orders placed on the BevMo website between August 2, 2018 and September 26, 2018. You are receiving this letter because our records indicate that you placed an order on the website during this timeframe.

What Information Was Involved

The malicious code may have captured the following types of information entered by customers on the BevMo website between August 2, 2018 and September 26, 2018: name, credit or debit card number, expiration date, CVV2 code, billing address, shipping address and phone number.

What We Are Doing

BevMo takes the privacy of our customers' personal information seriously and we deeply regret that this incident occurred. The service provider promptly removed the malicious code and engaged a third-party forensic firm to assist with investigating the incident. BevMo also took steps to address this matter after learning of the incident from the service provider, including by conducting our own independent investigation of this matter. We have also been in contact with law enforcement and the payment card companies, and will continue with our investigations into this matter. To help prevent something like this from happening again in the future, the service provider is continuing to review and enhance security controls and continuing to monitor its systems to further

detect and prevent unauthorized access.

What You Can Do

We want to make you aware of steps that you can take to help protect your personal information and guard against fraud and identity theft:

- **Checking Credit Reports and Financial Accounts**. You can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. You can also review your financial account statements to determine if there are any discrepancies or unusual activity listed. If you see anything you do not understand, call the financial institution immediately.

- **Reviewing Credit and Debit Card Account Statements**. You can carefully review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not recognize, you should immediately notify the issuer of the credit or debit card as well as the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

- **Consulting the Identity Theft Protection Guide**. Finally, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact us at 877-565-6276 between the hours of 9 a.m. to 9 p.m. Eastern time, Monday through Friday. Again, we sincerely regret any concern this incident may cause you.

Sincerely,

Tamara Pattison

Tamara Pattison

Chief Marketing and Information Officer

Information About Identity Theft Protection

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Security Freezes and Fraud Alerts: You have a 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.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-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 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a

spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

Additional Information for New Mexico Residents: New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You 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.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following: (1) the unique personal identification number, password or similar device provided by the consumer reporting agency; (2) proper identification to verify your identity; (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and (4) payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone. A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)
General Contact:
P.O. Box 740241
Atlanta, GA 30374
800-685-1111
Fraud Alerts:
P.O. Box 740256, Atlanta, GA 30374
Credit Freezes:
P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
General Contact:
P.O. Box 2002
Allen, TX 75013
888-397-3742
Fraud Alerts and Security Freezes:
P.O. Box 9554, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact:
P.O. Box 105281
Atlanta, GA 30348
800-888-4213
Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
888-909-8872