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 Breach

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

Chief Marketing and Information Officer

Information About Identity Theft Protection

Review of 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.

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.

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