quench
Water-as-a-Service™

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

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

Dear Quench Customer:

Quench USA, Inc. ("Quench") is writing to inform you of a recent event that may affect certain information related to your company. While we are unaware of any actual or attempted misuse of the information involved, out of an abundance of caution, we are providing you with information about the incident, steps we are taking in response, and steps you can take to protect against fraud should you feel it is appropriate.

What Happened? On February 13, 2017, we discovered our Coffee Service server had been infected with a virus that prohibited our access to our files. We restored the server and launched an investigation to determine the capabilities of the virus and how it was introduced to the server. On February 22, 2017, as part of our ongoing investigation, we determined this virus was introduced by an unknown third party that had access to a server on our information system and confirmed this server contains information relating to Quench Coffee Service customers.

What Information Was Involved? While our investigation is ongoing, we have no evidence the unknown third party accessed or acquired your company's information stored on the server. Nevertheless, we have confirmed this server housed information relating to your company, which may include your company's credit card number, expiration date, zip code and address. Out of an abundance of caution, we are providing notice of this incident to you given we cannot rule out unauthorized access to this information occurred.

What is Quench Doing? We take this matter, and the security and privacy of our customers' information, very seriously. In addition to launching an ongoing investigation and restoring the integrity of our information system, we are reviewing our policies and procedures and enhancing the security of our information system to mitigate the risk an incident like this will occur in the future. We are also providing notice of this incident to you.

What Can You Do? While we have no evidence your company's information was subject to unauthorized access, or that your company's information has been or will be misused, you can take steps to better protect against the possibility of identity theft and fraud by reviewing the additional information on protecting against misuse of your information. This additional information is included in the attached Privacy Safeguards.

For More Information. We understand you may have questions relating to this event and this letter. We have established a privacy hotline staffed with individuals familiar with this incident and how to better protect against the possibility of identity theft and fraud, and you can direct all questions and concerns to this line by calling 1-800-303-2887, between 9:00 a.m. and 6:00 p.m. ET, Monday through Friday, excluding major holidays.

We apologize for any inconvenience this incident may cause you, and remain committed to the privacy and security of our customers' information.

Sincerely,

Debbie Romano
Vice President of Customer Success
Quench USA, Inc.

PRIVACY SAFEGUARDS

We encourage you to remain vigilant against incidents of identity theft and financial loss by reviewing your account statements, your company's account statements and monitoring your credit reports for suspicious activity. Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit http://www.annualcreditreport.com/ or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

At no charge, you can also have these credit bureaus place a "fraud alert" on your credit file. A "fraud alert" will tell creditors to take additional steps to verify your identity prior to granting credit in your name; however, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the credit bureaus verify your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your files. You may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on your credit report.

You can also place a "security freeze" on your credit file that prohibits a credit bureau from releasing any information from your credit report without your written authorization but may delay, interfere with, or prevent the timely approval of any requests for new credit. If you have been a victim of identity theft, and provide the credit bureau with a valid police report, the credit bureau cannot charge to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You must contact each of the credit bureaus separately to place a security freeze on your credit file:

Equifax Security Freeze	Experian Security Freeze	TransUnion LLC
PO Box 105788	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-685-1111	888-397-3742	888-909-8862
800-349-9960 (NY Residents)	www.experian.com/freeze/center.html	www.transunion.com/securityfreeze
www.equifax.com/help/ credit-freeze/en_cp		

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. **For North Carolina residents,** the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov. This notice has not been delayed as a result of a law enforcement investigation.

Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.