IceMiller
LEGAL COUNSEL

One American Square | Suite 2900 | Indianapolis, IN 46282-0200

November 12, 2018

WRITER'S DIRECT NUMBER: (312) 726-2504
DIRECT FAX: (312) 726-2695
EMAIL: Nicholas.Merker@icemiller.com

VIA U.S. MAIL

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

Dear Sir or Madam:

Ice Miller LLP represents B.T.C.E., Inc. d/b/a HomeBrewIt.com ("HomeBrewIt"). We are writing to notify you of a security incident involving the personal information of seven (7) New Hampshire residents.

On or about March 7, 2018, HomeBrewIt discovered that on or about September 26, 2017, an unauthorized party was able to gain access to its hosting company's environment and execute malicious code on its website, HomeBrewIt.com. Although the hosting company assured HomeBrewIt that the breach had been secured, on or about October 1, 2018 the hosting company informed HomeBrewIt that they had failed to detect a second set of malicious code which had been installed on the website on September 26, 2017. Because the hosting company did not initially identify or remove this second set of malicious code, it remained on the website until or about October 1, 2018. As a result of the hosting company's failure to detect and remove the second set of malicious code, certain data remained exposed during that time frame. The compromised data may have included the name, address, and payment card information of seven (7) New Hampshire residents.

After HomeBrewIt discovered the incident, it advised the affected customers about the incident and the steps they can take to protect themselves from any harm that may result from the incident. HomeBrewIt has added security enhancements to the website to block points of entry the attackers used. The hosting company has implemented more robust monitoring tools to identify this type of breach and stop it from happening in the future. Furthermore, the hosting company has used third party tools to confirm that the site has now been entirely cleansed of malicious code. HomeBrewIt also has hired an outside penetration testing company to test the security measures of the site. HomeBrewIt continues to work with the hosting company to evaluate further security measures that can be added, and is even considering changing providers. HomeBrewIt's investigation into the incident is ongoing, and HomeBrewIt will continue to implement security enhancements as needed. We have no reason to believe that the personal information involved has been used to engage in identity theft.

Please direct any questions or requests for additional information to me.

Sincerely,

ICE MILLER LLP

Nicholas R. Merker

Enclosure: Template Notification

Attachment A
Template Notification

Date

Name
Address
Address
Address

Dear:

NOTICE OF DATA BREACH

Please read this letter in its entirety.

What happened?
I am writing to inform you of a security incident involving the hosting company of our website. We were initially made aware of this situation on March 7th, 2018. Our hosting company identified that an unauthorized party was able to gain access to its environment and execute malicious code on our website, HomeBrewIt.com.

Although we were assured the breach had been secured, on October 1st, 2018 it was discovered that there was a second set of malicious code not previously identified which has led to sensitive customer information being exposed. This latest code had a sophistication not seen before, and thus was not detected by the monitoring controls put in place by the hosting company.

What information was involved?
You are receiving this letter because you placed an order on our website using a credit card between March 7th and October 1st, 2018 and may have had your data compromised. The compromised data may have included your name, address and payment card information. In particular, we believe that your Credit Card number ending in ***XXXX*** may have been compromised. This number in conjunction with your billing address can potentially be used to make unauthorized purchases on your credit card.

While we have no evidence that any of your personal information was misused in any manner, we are taking appropriate precautionary measures to ensure your financial security and help alleviate concerns you may have.

What are we doing to address this situation?
Upon identifying the initial breach back in March, our hosting company immediately quarantined the primary piece of malicious code, and stopped any further leaking of information. Additional security enhancements were added to our website to block points of entry that the attackers used. The hosting company also implemented more robust monitoring tools to identify this type of breach and stop it from happening in the future. However, a secondary piece of malicious code has now been discovered. This code was added to the site around the same time of the initial breach, and the security enhancements added did not prevent this infection because the code was already there. We have been working closely with our hosting company to

deal with the situation, and are confident all malicious code has been removed from the site. The hosting company utilized a 3rd party tool to help them confirm that the site has been cleansed of malicious code. We are working with the hosting company to evaluate further security measures that can be added, and are even considering changing providers.

Because we value you as our customer, we are providing you with access to a dedicated fraud specialist via a toll-free number (1-800-405-6108) to assist you with any questions you may have concerning this matter. These services will be provided by **CyberScout,** a company that specializes in identity theft education and resolution. Please supply the fraud specialist with the following unique code when you call. <code>

In addition, we are offering you a **promotional code that will save you $10.00 on your next order.** The code can be redeemed with an order on our website www.Homebrewit.com, or via a Phone order by calling us at 574-295-9975. PROMOTIONAL CODE: <promo code goes here>

What you can do

We urge you to notify your issuing bank of this incident to inform them that your account may be at an increased risk for fraud so that your bank can flag your account. We also encourage you to monitor your accounts closely for any suspicious activity (future and past transactions within the last 7 months) and to notify your financial institution immediately if you notice any unauthorized transactions.

You may want to consider the following:

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to verify the identity of the applicant. If you choose to place a fraud alert, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)	**Equifax (1-800-525-6285)**	**TransUnion (1-800-680-7289)**
P.O. Box 4500	**P.O. Box 740241**	**P.O. Box 2000**
Allen, TX 75013	**Atlanta, GA 30374**	**Chester, PA 19016**
www.experian.com	www.equifax.com	www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.)
- **Upon receipt of your credit report,** we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to Quality Wine & Ale Supply/HomeBrewIt.com.

Other important information

You can obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC). The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft, or via postal mail at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

For more information
If you have any questions for us, please do not hesitate to call us at ***574-295-9975*** between 10-5 p.m. Eastern Time, Monday through Friday. You can also email us at customerservice@homebrewit.com.

Again, I am truly sorry about this situation. As a business owner, father of one (soon to be two!), and a credit card user myself, I understand how serious this is and the hassle this creates for you.

If for any reason you feel safer doing business with us over the phone, please do! We completely understand. Our phone orders go through a backend process that is protected by administrative passwords, so it is very secure. We can be reached at 574-295-9975. We will be glad to help you out!

We apologize for any inconvenience that this situation has caused.

Sincerely,

BRYAN JOHNSON
Second Generation Owner and President

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 22104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

You may also 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.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General. The Iowa Attorney General's Office can be reached at:

Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut street, Des Moines, IA 50319, (515) 281-5926, www.iowaattorneygeneral.gov

For residents of *New Mexico*:
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".

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, (503) 378-4320, www.doj.state.or.us

For residents of *Maryland, North Carolina,* and *Illinois*:
You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft

For residents of *Massachusetts*:
State law requires you be informed of your right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it

For residents of *Rhode Island*:
You have a right to file or obtain a police report related to this incident. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400.

For residents of all states:
Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is below.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze, also known as a credit freeze, is intended to prevent credit, loans and services from being approved in your name without your consent. With a security freeze in place, no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. As of September 21, 2018, there is no charge to place a security freeze on your credit report. To place a security freeze on your credit report, you need to make a separate request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
(800) 685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/freeze/center.html
(888) 397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19016
https://freeze.transunion.com
(800) 909-8872

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future. More information can also be obtained by contacting the Federal Trade Commission listed above.