Braintrust Software LLC dba The Braintrust Consulting Group
1678 Montgomery Highway South
Suite 104 #237
Hoover, AL 35216

January 15, 2020

Notice of Data Breach

Dear «Billing_Address_First_Name» «Billing_Address_Last_Name»,

We are contacting you regarding a data security incident that we suspect occurred at braintrustgroup.com. We have no direct evidence that any of your data was compromised, and are providing this notice to you out of an abundance of caution.

What Happened
In October of 2019, we identified and eliminated a malicious script on the checkout page of our website. The script was added to our website by an unauthorized third party, and went undetected despite our use of industry-standard malware scanning and anti-virus technology. We began investigating this incident immediately after suspecting a problem, and worked diligently to resolve it. We were able to locate and eliminate the unauthorized script and have fully restored our systems.

What Information Was Involved
We suspect that the malicious script may have been present on our website between October 21, 2019 and November 8, 2019, and may have compromised the data captured on the checkout page of our website, including names, addresses, email addresses, account passwords, and payment card information, including the payment card numbers, expiration dates, and card verification numbers of persons who placed orders on our site within this date range.

What We Are Doing
We have taken every step necessary to address and resolve the incident, and our systems have been restored and are operating with heightened system security. Additionally, we have taken steps designed to prevent this type of incident from recurring, including implementing heightened security in our checkout process.

What You Can Do

Customers whose information may have been involved should consider the following recommendations, all of which are good data security precautions in general:

- **Review Your Payment Card Account Statements.** We encourage you to remain vigilant by reviewing your payment card account statements. If you believe there is an unauthorized charge on your payment card, please notify the relevant payment card company by calling the number on the back of the card. Under federal law and card company rules, customers who notify their payment card company in a timely manner upon discovering fraudulent charges will not be responsible for those charges.

- **Order a Credit Report.** If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1.877.322.8228.

- **Review the Reference Guide.** The Reference Guide below provides additional resources on the protection of personal information.

We take the protection of your personal information very seriously and sincerely apologize for this incident and regret any inconvenience or concern this may have caused.

Sincerely,

Brian Rabon

Brian Rabon
CEO

REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1.877.322.8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Place a Fraud Alert on Your Credit File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

- Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241, 1.800.525.6285, www.equifax.com
- Experian, P.O. Box 9532, Allen, Texas 7501, 1.888.397.3742, www.experian.com
- TransUnion Fraud Victim Assistance Division, P.O. Box 2000, Chester, Pennsylvania 19016, 1.800.680.7289, www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

- Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241, www.equifax.com
- Experian, P.O. Box 9554, Allen, Texas 75013, www.experian.com
- TransUnion Fraud Victim Assistance Division, P.O. Box 2000, Chester, Pennsylvania 19016, www.transunion.com

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1.877.IDTHEFT (438-4338), www.ftc.gov/idtheft