Return to IDX:
PO Box 480149
Niles, IL 60714

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

July 24, 2023

Subject: Notice of potential impact to your cardholder data

Dear <<First Name>> <<Middle Name>> <<Last Name>>,

We are writing to notify you of a data security breach experienced by CommerceV3, a third-party e-commerce platform that Jack Stack Barbecue (Jack Stack) uses to process payment information for nationwide shipping orders via ship.jackstackbbq.com. Following a forensic investigation performed by CommerceV3, it appears that your payment information may have been involved in the breach. For the protection of your data, we ask that you read this letter carefully as it contains details about the incident and provides resources you may utilize to protect your information moving forward.

What Happened? On June 19th, 2023, Jack Stack Barbecue received notification from CommerceV3 that its forensic investigation, aided by third-party cybersecurity experts, was complete. Based on the results from that investigation, Jack Stack learned that a data security incident perpetrated by an unknown actor occurred inside CommerceV3's system sometime between November 24, 2021 and December 14, 2022, and that some Jack Stack customers may have been impacted.

What Information Was Involved? The information that may have been impacted includes your name along with your email address, billing address, payment card number, CVV code and expiration date for cards used on the Jack Stack website between November 24, 2021 and December 14, 2022. Neither Jack Stack nor CommerceV3 have any evidence that your card payment information has been misused.

What We Are Doing? We have been working closely with CommerceV3 to ensure that all Jack Stack customers who may be impacted are formally notified of the incident and given resources to assist them. We also conducted a thorough evaluation of our payment processing system and confirmed that this incident did not affect any Jack Stack internal systems. CommervceV3 worked alongside the major card brands and banks throughout the investigation and has implemented additional security measures to further protect the privacy of its valued customers.

What You Can Do? Following this letter you will find information about steps you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information: To help answer any questions regarding this incident, Jack Stack has established a dedicated call center through IDX. The call center can be reached at 1-888-220-5513 Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. IDX representatives are well-versed in the incident and can answer any questions you may have.

Thank you for your patience and understanding. We continue to work alongside CommerceV3 to ensure the security and privacy of personal information remains a top priority.

Sincerely,

Travis Carpenter
CEO + President
Jack Stack Barbecue

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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