14555

ISAAC'S
RESTAURANTS

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

14555

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notification of Data Security Incident

Dear <<Name 1>>:

We are writing to inform you of a data security incident that may have involved your payment card information. At Isaac's Restaurants, we take the privacy and security of your information very seriously. We are writing to inform you of the incident, and to advise you about certain steps that can be taken to ensure your information is protected.

What Happened? On November 21, 2018, we learned of suspicious activity on our third-party vendor's e-commerce web platform. Upon discovering the activity, we took immediate steps to further secure our system and conducted a thorough internal investigation to determine the scope of the problem. We also engaged a forensics firm to conduct an independent investigation into what happened and whether customer payment card information had been accessed or acquired without authorization.

What Information was Involved? On January 8, 2019, after an extensive forensics investigation and diligent review of the customer information that was affected, we determined that the incident may have involved the payment card information of customers who utilized the web platform to purchase products from October 18, 2018, through December 18, 2018. The affected payment card information may have included names, addresses, payment card numbers, expiration dates, and security codes.

What Are We Doing? As soon as Isaac's discovered the incident, we took the steps discussed above. In addition, we reported the matter to the payment card brands to protect your payment card information and prevent fraudulent activity. We have also reported the incident to local and federal authorities to hold the perpetrators accountable. We are providing you with information about steps you can take to protect your personal information. In order to prevent similar incidents from occurring in the future, we have implemented additional measures to enhance the security of our e-commerce web platform. In addition, we are providing you with Equifax Identity Restoration services at no cost to you. This service is automatically provided to you without the need to enroll. **Please keep a copy of this letter to provide as proof of eligibility to receive Equifax Identity Restoration.** In the event you experience identity theft, please contact the Equifax call center at 877-368-4940, 9:00 a.m. to 8:00 p.m. Eastern, Monday through Friday, before May 31, 2019.

What You Can Do: You can also follow the recommendations on the following page to protect your personal information. We recommend that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

For More Information: We remain committed to protecting your information. If you have any questions, please contact our dedicated call center at 877-208-9780, 9:00 a.m. to 9:00 p.m. Eastern, Monday through Friday.

Thank you for your loyalty to Isaac's and your patience through this incident. We take your trust in us and this matter very seriously. Please accept our apologies for any worry or inconvenience this may cause you.

Sincerely,

D. Michael Weaver
President and CEO
Isaac's Restaurants
354 N. Prince Street
Lancaster, PA 17603

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review 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 should also 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 (the "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 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 can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.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 90 days. 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. 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 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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies to 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.