



January 23, 2024

Notice of Data Breach

Dear Customer:

We are sending you this notification as a member of our Deli Dollars rewards program or holder of a Jason's Deli online account.

We, Deli Management, Inc. d/b/a Jason's Deli ("Jason's Deli"), are sending this in response to a data security incident that we recently became aware of and that possibly involved your personal information. You are receiving this notice to provide you with details of the incident – including the information that may have been accessed, the actions we have taken, and actions you may want to consider taking.

WHAT INFORMATION WAS INVOLVED

If the unauthorized party was able to access your account, they may have had access to your personal information stored in the account. That information may have included your name, address (including all saved delivery addresses), phone number, birthday, preferred Jason's Deli location, order history, contact lists (if any – names and email addresses used for sending group orders), house account number (if any), Deli Dollars points, available redeemable amounts and banked rewards, as well as truncated gift card/credit card numbers. The unauthorized party would not have been able to view your entire payment/gift card number – potentially they would only have been able to view the last four digits.

WHAT WE ARE DOING

Once Jason's Deli learned of the incident, we began acting to protect the accounts, which included working to identify any potentially affected accounts and requiring that passwords to the accounts be more complex. If we have not already done so, we intend on restoring customers' Deli Dollars account balances, where applicable. As always, we continue to take data security seriously and our fraud controls will remain ongoing as appropriate in order to minimize the risk of any future incidents.

WHAT YOU CAN DO

Please change the password to your Jason's Deli account as soon as possible. You can do so by clicking the link or entering the following web address into your browser: <https://cms.jasonsdeli.com/password-reset>. Please use a password that is not easy to guess and one that is not used on other websites or accounts. You should also change your username and/or passwords for all other online accounts for which you used the same username, email address and password.

The enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to remain vigilant against potential identity theft and fraud by carefully reviewing your account statements and free credit reports for suspicious activity and to detect errors.

Reference Guide

Review Your Account Statements

Carefully review account statements and credit reports to ensure that all of your account activity is valid. Report any questionable charges promptly to the financial institution or company with which the account is maintained.

Order Your Free Credit Report

To order your free annual 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 ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

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 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