NOTICE

This notice is provided pursuant to Section 899-aa of the New York General Business Law.

In providing its customers with the highest quality food and service possible, LJZ Enterprises Inc. d/b/a Sinatra's Restaurant ("LJZ") collects and retains electronic data in the ordinary course of its business. LJZ uses commercially reasonable measures to protect such data from loss or unauthorized access, disclosure or use. Despite these measures, some of LJZ's electronic data may have recently been illegally acquired by a hacker.

A third party may have gained unauthorized access to data contained on the point of sale system of LJZ on November 27, 2016 (the "Breach"). The Breach, which was discovered on December 7, 2017, may have resulted in the hacker acquiring customer credit card and security code numbers.

All customers using credit cards at LJZ's restaurant from November 27, 2016 to December 27, 2017 may have been affected by the Breach. These customers are urged to pay particular attention to their credit card account statements for unauthorized charges or other unauthorized transactions. They may also want to review, and take the additional steps set forth in, the section of this notice entitled ***Information about Identity Theft Protection***.

Promptly after learning of the Breach, LJZ retained Avalon Legal, a data security consulting firm with offices in Buffalo, New York. The consultant (1) analyzed the details of the Breach, (2) assisted LJZ in terminating the Breach, and (3) assisted LJZ in taking steps to reduce the probability that a similar breach will occur in the future. In particular, with the assistance of the consultant and LJZ's computer vendor, LJZ has replaced its point of sale system and implemented other technical enhancements to reduce the probability that a similar breach will occur in the future.

LJZ deeply appreciates its customers and wants them to be confident in its ability to securely hold their personal data. All personal data held by LJZ is, and always has been, as safe with LJZ as it reasonably can be in today's world. As everyone knows from other well-publicized security breaches, no electronic data is completely safe from the criminal activity of hackers. Every day there are additional accounts of businesses, both large and small, and government agencies having their systems and data compromised. Having said that, LJZ completely understands that unauthorized access to a customer's personal data in LJZ's possession may cause legitimate concern.

LJZ currently has no reason to believe that any personal data has been used by a third party without authorization as a result of the Breach, but LJZ continues to monitor the situation. If LJZ subsequently has a reasonable basis to believe that, due to the Breach, any personal data is being used by a third party without authorization, LJZ will update this notice and help protect such personal data. Similarly, if customers experience any suspicious activity regarding their credit card account that may be related to the Breach, you should immediately notify LJZ at (716) 877-9419 or mike@sinatraswny.com.

Information about Identity Theft Protection

It is recommended that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may 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. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, GA 30374-0241, 1-800-685-1111, or www.equifax.com

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

TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, or www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

You should remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft as follows:

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

For residents of New York:
Office of Attorney General's Office
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/consumer-frauds-bureau/identity-theft

Fraud Alerts

There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an

extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008 (or see www.equifax.com)
Experian:	1-888-397-3742 (or see www.experian.com)
TransUnion:	1-800-680-7289 (or see www.fraud.transunion.com)

Credit Freezes

You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a personal identification number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws and the fees that can be charged for placing, temporarily lifting, and removing a credit freeze vary from state to state. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348 (or www.equifax.com)
Experian:	P.O. Box 9554, Allen, TX 75013 (or www.experian.com)
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000 (or see www.freeze.transunion.com)

You can obtain more information regarding fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee to place a freeze or lift or remove a freeze.