Davis Wright Tremaine LLP

Suite 2200
1201 Third Avenue
Seattle, WA 98101-3045

November 23, 2011

Via first class mail
Via fax: 603.271.2110

The New Hampshire Office of Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Dear Sir or Madam:

Pursuant to N.H.R.S.A. § 359-C:20(I)(b), I am providing this notice to you that the credit or debit card information of approximately 229 New Hampshire residents was obtained by thieves from the credit card processing system used in one or more Jetro/Restaurant Depot stores. Jetro plans to notify the affected individuals by sending the enclosed notice to them by first class mail on Monday, November 28, 2011. Information regarding the security breach, the information stolen, and steps Jetro/Restaurant Depot has taken to respond to the theft are described in the enclosed notice. Please let me know if you have any questions regarding this matter.

Very truly yours,

Davis Wright Tremaine LLP

Randy Gainer

Enclosure

c: Stanley Fleishman, CEO, Jetro/Restaurant Depot
Richard Kirschner, COO, Jetro/Restaurant Depot

[Jetro/Restaurant Depot letterhead]

November 28, 2011

«first name» «last name»
«address1»
«address2»
«city», «state» «zip»

Dear [name or] Valued Customer:

We recently determined that computer hackers stole credit and debit card information from the card processing system we use in our stores. The thieves obtained the card information as it was being processed. You are receiving this letter because we believe your credit or debit card information was stolen. This letter explains actions we have taken in response to the theft and describes some actions you can take to protect yourself against fraud.

The stolen information: Computer forensic investigators we hired to investigate the theft currently believe that the thieves obtained the names of cardholders, credit or debit card numbers, card expiration dates, and verification codes that were on the magnetic stripes of credit and debit cards used at our stores from September 21 through November 18, 2011.

How the thieves stole the card information: The investigators determined that the thieves inserted malicious software or "malware" into the credit and debit card processing systems we use in our stores. The malware collected card information as it was processed, stored it temporarily, and then sent it to a computer server in Russia.

Actions we have taken: We learned on November 9 that some our customers had experienced credit card fraud after they used their cards at our one of our stores. We hired Trustwave, a leading computer forensic firm, on November 10 to investigate. By November 18, Trustwave investigators had identified the malware and blocked the mechanisms they discovered by which the thieves exported card information from the card processing system. At this time, Trustwave investigators continue their investigation and they will take any necessary additional steps to eliminate the threat caused by the malware. Trustwave and our Information Technology staff reviewed the safeguards we use to protect card information and made appropriate changes to improve the security measures we use to protect card information.

We notified all the major card brands and provided information about potentially compromised accounts. The card brands, in turn, notified card-issuing financial institutions who can take steps to protect cardholders through enhanced fraud monitoring or by reissuing cards.

Actions you should take: To protect yourself from possible fraudulent charges, you should contact officials at your card issuer immediately by calling the toll-free number on the back of your card or on your monthly statement, tell them you have received this letter, and ask them to cancel and reissue the card. You should also closely review the statements for any credit or debit card you used at one of our stores between September 21 and November 18, 2011. You should immediately notify the bank or financial institution that maintains the card account of any unauthorized charges. Most banks or financial institutions will reimburse your account for any fraudulent charges.

You should refuse to provide information to anyone who calls or emails you to ask you for confidential information. Such calls and emails are known as "phishing." Fraud perpetrators may ask you for bank account information, credit card numbers, or your PIN. Banks and legitimate businesses will not call or email you to ask for such information.

You can contact one of the three major credit reporting agencies at:

Equifax Fraud Reporting
1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

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

TransUnion Fraud Reporting
1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

Additional information, including information about how to prevent identity theft, is available from the Federal Trade Commission (FTC). You can contact the FTC at 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.consumer.gov/idtheft or 1-877-438-4338. If you become a victim of identity theft, you should report it to the police.

Reimbursement and other services we will provide: If you are required to pay any fraudulent charges on your credit or debit card, or if your bank charges you a fee to replace your credit or debit card, or if the theft of your card data from the card processing system we use causes you to have to pay any other costs, please contact ID Experts® at the number below. We have contracted with ID Experts to provide counseling and recovery services to our customers who have been affected by the theft. ID Experts, and possibly an insurance investigator, will investigate any costs you incur due to the theft that are not reimbursed by your bank. Jetro/Restaurant Depot will reimburse you for any such costs you reasonably incur, either through insurance it has purchased or directly.

We are also offering you a membership in ID Experts' FraudStop™ Basic Edition, at our expense. The membership provides individuals with 12 months of benefits. ID Experts will keep FraudStop members up-to-date on new identity theft scams, tips for protection, legislative updates, and other topics. Members will also have access to the ID Experts' team and the online resource center for news, education, and advisory services.

Contact number for assistance and further information: Representatives from ID Experts have been fully informed about the card information theft at Jetro/Restaurant Depot. They can answer your questions and respond to concerns you may have regarding the theft. They are available to assist you and to enroll you in the FraudStop program Monday through Friday from 9 a.m. to 9 p.m. Eastern Time. You can reach them by calling **1-877-819-8914**. Please have your Jetro/Restaurant Depot membership number available. You may also register for the free ID Experts FraudStop membership by visiting www.idexpertscorp.com/J-RDEnroll.

Maryland and North Carolina Residents can obtain additional information about preventing identity theft from:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
Telephone: 1-888-743-0023

Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com/
Telephone: 1-919-716-6400

We regret any inconvenience or concern the theft may have caused you.

Sincerely,

_____