Cruzstar LLC.
453 Lincoln St.
Suite 102
Carlisle, PA 17013

March 6, 2018

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General:

We are a software company named Cruzstar LLC. based in Carlisle, PA. We create shopping cart software for restaurant merchants. We are writing to notify you of a security incident involving New Hampshire residents.

On November 28, 2017, we identified unauthorized access to our computer network. We immediately began an investigation and notified Federal law enforcement of the incident. Although the investigation did not identify evidence of unauthorized access to payment card data, we determined that the potential for that to have occurred existed for certain software version and transactions. Findings from the investigation suggest that, for customers who placed or attempted to place orders on our Desktop website from November 5, 2017 to November 28, 2017, information associated with the order being placed, including the customer's name, address, payment card number, expiration date and security code (CVV), may have been obtained by an unauthorized third-party. There were approximately 76 consumers who may be New Hampshire residents and who may be impacted.

Beginning February 20, 2018, we provided written notification to our New Hampshire restaurant merchants. The notification recommended that they notify their patrons and follow state notification requirements. We also provided a telephone number for affected merchants to call with any questions they may have. Included is a sample notification that we are providing to our restaurant merchants to use for their patrons.

To help prevent this type of incident from happening again, we are continuing to take steps to strengthen the security of our network.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Adrian Fang
Partner

Dear Valued Customer:

We recently identified and addressed an incident that may have affected the security of your payment information. Last year in 2017, only our Desktop online ordering site was attacked and injected with malware intended to capture credit card information while it was being submitted. Upon discovery, our online ordering provider conducted an investigation and took immediate steps to contain and remove the malware. As part of their investigation, they engaged a leading cybersecurity firm that assisted them with the investigation. In addition, they also notified Federal law enforcement of the incident and are working closely with the major credit card brands to ensure the incident was properly addressed. We sincerely apologize for any inconvenience this incident may cause you.

Who is impacted

Our online ordering provider's cybersecurity team has determined that the timeframe of this incident was from November 5, 2017 to November 28, 2017 and impacted only certain transactions. They have learned that the malware was contained to ONLY the Desktop online ordering site that you used during that time frame. Your payment information such as card number, expiration date, address, zipcode, and security code (CVV) may have been obtained by an unauthorized third-party. We are notifying you because you placed or attempted to place an order on our Desktop online ordering site during this time period.

What we are doing

We take the security of credit card and other personal information very seriously. Our online ordering provider is using automated tools to help identify any suspicious activity. Furthermore, to prevent this from happening again, they are actively working with leading security experts and law enforcement to strengthen the security of their network.

What you can do and additional information

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at www.annualcreditreport.com, calling toll-free 1-877-322-8228, or 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 any of the credit reporting agencies below:

Equifax
PO Box 740241
Atlanta, GA 30374
www.equifax.com
888-766-0008

Experian
PO Box 9554
Allen, TX 75013
www.experian.com
888-397-3742

TransUnion
PO Box 2000
Chester, PA 19016
www.transunion.com
800-680-7289

If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission ("FTC"). You also may contact the FTC to obtain additional information about avoiding identity theft.

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

State Attorneys General: Information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/whos-my-ag.php.
You may obtain information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or credit freeze on your credit report.

If you have further questions about this incident, please call our online ordering provider's hotline toll-free at 888-358-7211.