John S. Wagster
Member
615.251.5586
jwagster@fbtlaw.com

July 19, 2016

VIA CERTIFIED MAIL

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

Dear Attorney General Peterson:

Pursuant to N.H. STAT. ANN. §359-C:20, I am writing on behalf of my client CiCi Enterprises, LP, 1080 West Bethel Road, Coppell, Texas 75019, to notify you of a breach of security potentially impacting an unknown number of New Hampshire residents.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

While this matter is still under investigation, we wish to report what we currently know. In early March of 2016, we received notice from several of our restaurant locations that their Point of Sale (POS) systems were not working properly. The POS Vendor immediately began an investigation to assess the problem and initiated heightened security measures. When the Vendor found malware on the POS software at some of our restaurants, we began a restaurant by restaurant review and remediation. We also retained a third party cyber security firm to perform a forensic analysis to determine what, if any, information might have been compromised and to verify that all threats have been eliminated. The forensic firm reported its findings on July 19, 2016 confirming that a malicious software program had been introduced to our system by a hacker on the POS software used by some of our restaurant locations. The threat of that malware to our restaurants has been eliminated.

The report revealed that payment card information may have been compromised from payment cards used at certain of Cicis' restaurants. Of those restaurants, the vast majority of intrusions began in March of 2016 and the threats were eliminated on a store by store basis through July of 2016. A smaller percentage of affected restaurants had intrusions dating back to 2015. While we believe most of the breaches were remedied within a few weeks of the intrusion, out of an abundance of caution we are not declaring some restaurants as threat-free until they were reviewed by our forensic analyst this month. A list of the impacted locations is attached. Not all payment cards used at the affected restaurant locations were compromised; however, some information from some payment cards used in such locations may have been accessed by the malware. No other customer information was compromised.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

As demonstrated by the attached list, we believe no store(s) in New Hampshire were impacted. Because Cicis does not have sufficient information to determine which payment cards used during the relevant time-frame were accessed, we are not currently able to determine how many individuals were impacted. Moreover, because Cicis' system does not retain addresses for payment card users, we are not currently able to determine which, if any, New Hampshire residents were affected. As such, this notification is being made out of an abundance of caution.

STEPS CICIS HAS TAKEN OR PLANS TO TAKE RELATING TO THE INCIDENT

As part of our response to this incident, we have notified law enforcement and the state agencies as required by the laws of the jurisdictions in which our restaurants are located, and we will continue to assist with their investigation. The payment card networks have also been informed so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used during the timeframe in which cards may have been compromised. Cicis continues to monitor and upgrade our systems to keep your information as secure as possible.

We are also posting the attached notification on the homepage for Cicis website on July 19, 2016. Additionally, e-mails will be sent to potentially impacted members of Cicis loyalty program, none of which reside in New Hampshire.

OTHER NOTIFICATION AND CONTACT INFORMATION

If you have any questions or need further information, please contact me. I can be reached at 615.251.5586. My email address is jwagster@fbtlaw.com.

Very truly yours,

FROST BROWN TODD LLC

John S. Wagster

0125594.0637411 4815-9325-6243v1