yummie
BY HEATHER THOMSON

STATE OF NH
DEPT OF JUSTICE
2016 NOV 18 PM 12:01

November 16, 2016

Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

We write to inform the Consumer Protection and Antitrust Bureau of a data security incident that we have just uncovered, which involved personal information of some of our customers. Between October 4, 2016 and November 1, 2016, malicious "credit card skimming" software was installed by an unauthorized foreign party on the front end of our website, www.yummielife.com, without our knowledge or consent. The personal data which was illegally diverted included the names, billing addresses, credit card numbers, expiration dates and card security/access codes, and user names and passwords of some of our customers. Approximately 7 residents of New Hampshire were affected by this incident and they will be notified by us on November 17, 2016.

The timeline of events is as follows:

- On October 31, we received information suggesting that fraudulent charges were made to a customer's credit card after placing an order at http://www.yummielife.com.
- On November 1, as we investigated the particular complaint, our website service provider, Something Digital, discovered a compromised Magento user account (michelle), which had uploaded a malicious script into the System > Configuration > Design > Footer > Miscellaneous HTML section of the Magento admin on Oct 4, 2016 9:13:20 PM.
- From the data we have access to, Oct 4, 2016 9:09:28 PM was the first recorded login from this account (IP address 149.154.158.51).
- Over the past month, this account has been accessed from three different IP addresses (149.154.158.51, 50.7.71.93, and 176.215.13.29) with the primary IP (176.215.13.29, located in Russia) being the most frequent.
- Through search of available access logs, Something Digital located requests from the primary IP to files on the server that likely functioned as points for the attacker. (Note: Something Digital currently has access to one month of Apache access logs, but we have determined to obtain an additional 2 months of access from Rackspace to review.)
- Something Digital located three seemingly malicious files in the WordPress uploads directory `/blog/wp-content/uploads/2016/` (index.php, ee.php, and linuxprivchecker.py).
    - Something Digital has not de-obfuscated the PHP scripts, but the Python script is a tool to check for privilege escalation vulnerabilities. We saw evidence in the logs that `index.php` had been accessed via the web on Oct 4 just before `/downloader/` (a public admin login URL page from default Magento admin) was accessed.
    - We found a third PHP script in the Magento media directory at `media/tmp/shs.php`. This script was a backdoor into the server and was accessible via the browser without

yummie
BY HEATHER THOMSON®

any authentication. This script was accompanied by two empty files (shs.php.permission-backup and .shs.php.bnQSQz.permission-backup).

As soon as we discovered this security breach on November 1, 2016, we immediately took action to remove the credit card skimming software and eliminate any further exposure. Specifically, the following steps were taken:

- Something Digital removed the malicious script from Magento's Miscellaneous Footer HTML;
- Something Digital removed affected code from the server;
- Something Digital immediately changed the password for and deactivated the `michelle` user account;
- Yummie removed old, unused user accounts and changed passwords for remaining accounts (client managed);
- Something Digital disabled the /downloader directory (admin login);
- Something Digital disabled /var directory (cacheleak);
- Something Digital disabled directory indexing;
- Something Digital upgraded WordPress;
- Something Digital blacklisted IPs that were attempting to access admin;
- Something Digital whitelisted admin-authorized external IPs;
- Something Digital changed the Magento admin route;
- Something Digital locked the WordPress blog to prevent admin access; and
- Something Digital requested site backups from Rackspace to further investigate issues.

We have also reported this incident to the Federal Bureau of Investigation and will provide them and the Consumer Protection and Antitrust Bureau any information and assistance we can to identify the hackers. Notification to our customers was not delayed because of a law enforcement investigation. A copy of the notice that will be sent to our New Hampshire customers is attached hereto.
Please let us know if we can provide any additional information or be of any assistance to the Consumer Protection and Antitrust Bureau in connection with this data breach incident.

Sincerely,

Richard Rothfeld
General Counsel
Times Three Clothier, LLC dba Yummie by Heather Thomson