RECEIVED
DEC 20 2019
CONSUMER PROTECTION

Christopher DiIenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

December 16, 2019

VIA FIRST CLASS U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Laudisi Enterprises Inc. d/b/a SmokingPipes.com ("Laudisi"), located at 550 Highway 9 East, Longs, South Carolina 29568, and are writing to notify you of a recent incident that may affect the security of the personal information of approximately four (4) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Laudisi does not waive any rights or defenses.

Nature of the Data Event

On November 18, 2019, Laudisi discovered a malicious code was present on the checkout page of its e-commerce website, SmokingPipes.com. Laudisi immediately removed the malicious code and launched an investigation to determine how the code was placed on the checkout page and what information may have been affected as a result. Laudisi's investigation determined that the malicious code gathered certain payment card information as it was manually entered on the checkout page and sent that information to an external site.

The investigation determined that this event impacted a total of 722 customers who manually entered their payment card information on the checkout page between November 13, 2019 and November 18, 2019.

The types of information captured by the malicious code included customer name, payment card number, expiration date, and security code or CVV number.

Notice to New Hampshire Residents

On November 22, 2019, Laudisi sent notice of this event via email to all impacted customers, including four (4) New Hampshire residents, providing a description of the event, the type of information involved, what SmokingPipes.com was doing in response, and what individuals can do to protect their information. Such notice was provided in substantially the same form as the letter attached here as ***Exhibit A.***

Other Steps Taken

Laudisi is providing potentially affected individuals with information on how to protect against identity theft and fraud, including monitoring financial accounts for suspicious activity and information on how to contact the Federal Trade Commission and law enforcement to report any attempted or actual identity theft and fraud. In addition to providing notice of this incident to you, Laudisi will be providing notice to other state regulators.

Since learning of this incident, Laudisi has added IP tracking capabilities to help detect unauthorized activity on its website, implemented security features around the form fields in the checkout page and elsewhere, began running nightly searches for malicious code on its systems, and added two-part authentication to its business systems, in order to prevent similar future incidents.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me at (267) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD:KML
Enclosure

Exhibit A

SMOKINGPIPES

FRESH PIPES SERVED DAILY

Dear [FNAME] [LNAME],

I am writing to inform you that your credit card information (including your credit card number) was exposed to theft during checkout at Smokingpipes.com.

This breach was of very limited scope with 722 users of the website affected, representing less than one half of one percent of our customers. Still, if you're receiving this email, you were one of those few hundred who we failed in our security efforts and we are very sorry.

There is a detailed explanation of this below, but here's the brief version: On the morning of Wednesday, November 13th, a hacker was able to access Smokingpipes.com's business systems for approximately two hours before we noticed the intrusion and blocked his access. We began assessing the damage. The following Monday (November 18th), we found malicious code that the hacker deposited in our content management system. We eliminated it immediately. Further work analyzing the software revealed that it was designed to gather credit card information as it was being entered on the client (your) browser.

We never store your credit card information. The hacker intercepted your information before it was encrypted and sent to our server, and a copy of that information was diverted to a server that he controls.

Fortunately, we know exactly which customers were exposed. Only certain types of transactions on Smokingpipes were affected, and only for those five days. Once we detected the malicious code we removed it immediately. We also implemented a series of new security measures to better protect Smokingpipes.com and our customers.

You are receiving this email because your credit card information was exposed. We have reported this event, but we suggest that you contact your card issuer.

Again, we are deeply sorry that we failed to properly safeguard your information. If you have any questions or would like to talk to us about what's happened, please feel free to reach out to us at info-priority@smokingpipes.com.

Sincerely yours,

F. Sykes Wilford

A more detailed and specific synopsis:

We experienced a persistent DOM based cross-site scripting attack using a JS file called from an insertion in our CMS manager. Access to our CMS systems was achieved through a non-persistent DOM based XSS attack that hijacked the session of an employee of Smokingpipes.com.

The cross-site javascript call was inserted in a varchar type field that holds the label for the credit card box on the checkout page. It copied the DOM from the client, including credit card information, and pushed it to a third party.

The exploit existed for roughly five days, from Wednesday, November 13th, at 10:40am to Monday, November 18th, at 4:10pm.

While it took us less than two hours to detect the intrusion and block the intruder (IP was blocked, credentials for that user changed, all sessions reset and all user passwords were changed), it took longer to uncover the damage done. On November 18th, the exploit was discovered and closed.

We de-obfuscated, analyzed and deployed a neutered version of the malicious JS code in a test environment over the following two days.

We determined to a great degree of certainty that it had indeed succeeded in its goal to collect and send the data, as we were able to pass dummy credit

card and billing data through it to a third party (a test server, in this case) successfully.

Since these were transactions of a specific sort during a clearly defined time span (credit cards only and only when saved payment methods were not used) we were able to determine exactly which users were affected.

At this point, we are certain that we understand the full scope of the exploit, both in terms of users affected (722 in all) and exactly what information was passed.

Hours of operation:
Monday-Friday: 9am-9pm EST
Saturday: 10am-5pm EST
Sunday: 12pm-4pm EST

Smokingpipes.com
550 Hwy 9 E
Longs, SC 29568
888.366.0345
info-priority@smokingpipes.com