EDWARDS WILDMAN

EDWARDS WILDMAN PALMER LLP
20 CHURCH STREET
HARTFORD, CT 06103
+1 860 525 5065 main +1 860 527 4198 fax
edwardswildman.com

Karen L. Booth
+1 860 541 7714
fax +1 888 325 9526
kbooth@edwardswildman.com

Federal Express

January 29, 2013

Attorney General Michael A. Delaney
New Hampshire State Attorney General's Office
33 Capitol Street
Concord, NH 03301

Re: Stethoscope.com LLC
Notification of Potential Security Breach pursuant to N.H. Rev. Stat. § 359-C.20

Dear Attorney General Delaney:

We write to advise you of an incident involving potential unauthorized access to personal information of New Hampshire residents. The webserver used to host the website of our client, Stethoscope.com LLC (the "Company"), a small Massachusetts-based Internet retailer, was recently accessed by an unidentifiable hacker, resulting in unauthorized access to and potential acquisition of personal information of 164 residents of New Hampshire, as further described below.

Learning About the Incident. During routine server maintenance on the evening of December 12, 2012, the Company's independent contractor web programmer discovered that unauthorized scripts had been uploaded to the Company's web server, which is hosted by national third party provider, RackSpace. On December 16, 2012, the Company learned that the personal information of New Hampshire residents may have been exposed in connection with this incident.

The forensic investigation to date has revealed that an initial malicious script was placed on the Company's server on November 27, 2012. The attacker ran a secondary script on the server on December 3, 2012. The secondary script that the hacker ran on December 3, 2012 resulted in the potential access to and acquisition of customer names, addresses, email addresses, decrypted credit card numbers, and credit card expiration dates and security codes. The database did not contain Social Security numbers, drivers' license or other government-issued identification numbers; thus, no such additional information was exposed in connection with this incident. Although the credit card numbers were stored using 256-bit encryption, the forensic investigation to date revealed that the attacker was able to decrypt the card numbers on December 3, 2012 using the secondary script.

The forensic investigation to date revealed that the attacker accessed decrypted credit card numbers on December 3, 2012, although the initial script was present on the Company's server from November 27, 2012 until December 12, 2012. The Company deleted both unauthorized scripts immediately upon learning of their existence on December 12, 2012, which, in combination with other security actions taken by the Company on that date, effectively curtailed this attack.

EDWARDS WILDMAN

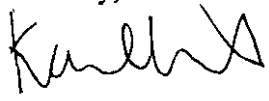
Upon discovery of the incident, the Company took the following actions: (i) took immediate remedial actions to further enhance security; (ii) filed a complaint with the Natick, Massachusetts Police Department and federal law enforcement via the Internet Crime Complaint Center (IC3); (iii) investigated the situation; (iv) engaged our law firm to oversee forensics, coordinate appropriate data breach response, and advise on legal obligations under applicable law; (v) engaged a third party forensic firm to investigate the incident to determine the extent of the unauthorized access or acquisition and to advise the Company regarding remediation and security enhancement measures; (vi) notified its credit card processor, which indicated that it would notify MasterCard and Visa; (vii) notified American Express and Discover; and (viii) notified Equifax, Experian and TransUnion regarding this incident. The forensic investigation regarding this matter is continuing.

Communicating with Affected Individuals. In order to ensure that affected individuals resident in New Hampshire may take steps to protect themselves from possible fraudulent charges, the Company will provide notice regarding this incident via first class mail on or about January 31, 2013. The notification materials, a template of which is enclosed with this letter, advise customers to remain vigilant by reviewing account statements and monitoring free credit reports. The notifications materials also offer call center support to affected individuals.

Efforts to Deter Future Breach. The Company has taken several important steps to improve the level of its data security following this incident, including the following: (i) reconfigured its system to no longer store full credit card numbers or security codes, even in encrypted form; (ii) upgraded software; (iii) modified its firewall policies to further restrict access; (vi) implemented additional access control restrictions on its server; and (v) increased the profile of data security issues within the Company.

We trust that this letter and its enclosures provide you with the information required to assess this incident and the Company's response. Please let us know if you have additional questions or if we may be of further assistance.

Sincerely,



Karen L. Booth

Enclosure

AM 18061356.1

{Mail Date}

{Full Name}
{Street Address}
{City, ST ZIP+4}

Re: Important Notice Regarding Credit Card Account Ending in XXXX.

Dear Name:

It is with regret that I write you today regarding a data security incident. During routine server maintenance in mid-December, we learned that on or about December 3, 2012, a hacker gained unauthorized access to the webserver used to host our website, resulting in the potential acquisition of your name, address, e-mail address, and information related to your credit card identified above, which you used to purchase merchandise through our website. The credit card information exposed included your credit card number, expiration date and security code. The credit card numbers were protected using 256-bit encryption; however, it appears that the hacker was able to access this information.

We are writing to inform you of the data intrusion incident and the steps we have been taking to help safeguard your personal information. Upon learning of this incident, we took the following actions: (1) notified the credit card companies and local and federal law enforcement; (2) engaged a forensic investigation firm to investigate the situation; (3) determined what information had been compromised; (4) committed to notify affected individuals; and (5) took immediate remedial actions to further enhance security.

As always, we recommend that you remain vigilant and review your account statements and credit reports regularly. You can request a copy of your credit report free of charge through www.annualcreditreport.com. We have established a dedicated call center to answer questions about this incident. If you have any questions regarding this incident, please contact the call center at **(877) 288-8057** from 9:00 a.m. to 9:00 p.m. Monday through Friday, and 12:00 p.m. through 8:00 p.m. Saturday and Sunday, Eastern Time. Please note that the reverse side of this letter contains additional useful information regarding steps you can take to protect yourself from identity theft.

We take seriously our obligation to protect our customers' information, and we regret any inconvenience or concern that this incident may cause.

Sincerely,

Paul S. Paresky
President

U.S. State Notification Requirements

For residents of California, Hawaii, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, West Virginia, and Wyoming:

We are required by state law to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-888-4213
www.transunion.com

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State law advises you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Maryland and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about steps you can take to avoid identity theft.

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

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

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

For residents of Puerto Rico:

You can obtain information the Federal Trade Commission at www.ftc.gov/bcp/edu/microsites/idtheft/ regarding steps you can take to avoid identity theft.

For residents of West Virginia

You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to each consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a small fee to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse is a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion (FVAD)
P.O. Box 6790
Fullerton, CA 92834
www.transunion.com

For residents of Illinois

You may obtain information about fraud alerts and security freezes from the Federal Trade Commission at the contact information provided above and the following consumer reporting agencies:

Equifax
P.O. Box 740241
Atlanta, Georgia 30374
www.equifax.com
1-877-478-7625

Experian
P.O. Box 2104
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion (FVAD)
P.O. Box 6790
Fullerton, CA 92834
www.transunion.com
1-800-680-7289

You are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity for 12 to 24 months.