SUSAN MERRITT-GLENNY
Attorney At Law
477 Main Street, Suite #2
P.O. Box 105
Yarmouthport, Massachusetts 02675

ALSO ADMITTED IN CONNECTICUT
Telephone: (508) 362-5755
Email: Merrittesq@verizon.net

Facsimile: (508) 362-5756

July 1, 2014

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

Via Facsimile Only

Re: Security Breach Notification Letter

Dear Attorney General Foster:

We are writing to notify you of an apparent breach of security and additionally unauthorized access to and/or use of sensitive and possibly personal information occurring on the Dennis East International, LLC, ("DEI"), website. DEI's website is hosted by a third party, Omeganet of Georgia. Use of DEI's website is restricted to retailers.

Apparently, Omeganet's server was hacked. Omeganet reports the following two incidents. The first incident affects some customers who placed orders on the DEI website between June 1, 2014 and June 13, 2014. Omeganet reports that some customers ordering during this time period may have received a "phishing" email that requested credit card information.

In the second incident, Omeganet a/k/a CAMEO EZ, reports that their system was hacked affecting customers placing orders on the DEI website between May 28, 2014 and June 13, 2014. Omeganet reports that the hacker obtained the information in the order including the following: User ID (the number the Omeganet uses to identify the customer); Credit Card name; Credit Card number; Credit Card expiration date; Customer name; Customer email address, telephone number and billing and shipping address. Again, all customers using this website are required to be retailers.

It appears that one (1) New Hampshire customer will be notified of these incidents via the attached letter. The letter will be sent via email and USPS first class mail today.

Omeganet has assured DEI that they have remedied the problems and that they are taking all reasonable precautions to help prevent such incidents from occurring in the future.

If you require additional information on this matter please call me.

Sincerely,

Susan Merritt-Glenny

July ---, 2014

Customer Name
Address
City, ST

Dear_____:

We value your business and respect the privacy of your information. We are writing to let you know about a recent breach of security and possible acquisition or use of your personal information on DEI's website that is administered by a third party provider, Omeganet, of Georgia.

Incidents

Omeganet has recently informed DEI of the following two incidents.

The first incident affects some customers who placed orders on the DEI website between June 1, 2014 and June 13, 2014. These customers may have received a 'phishing' email that appeared to be from CAMEO EZ, looking for credit card information. This email was not from Omeganet and it was not from DEI. Omeganet has identified the problem and has made security changes to prevent further problems.

The second incident affected customers ordering on the DEI website between May 28, 2014 and June 13, 2014. Omeganet reports that their computer system was hacked, resulting in the hacker obtaining all information contained in the order including the following: User ID (the number the CAMEO EZ system uses to identify the Customer); Credit Card name; Credit Card number; Credit Card expiration date; Customer name; Customer email address; Customer telephone number; and Customer billing and shipping address.

Omeganet has assured DEI that they have contained the security breaches. Omeganet has informed DEI that they are working with a security expert and they have taken a number of steps to help prevent an unlawful intrusion like this from happening again.

It is recommended that you promptly contact your credit card company regarding this matter. Additionally, it is also recommended that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-IDTHEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Please also review the attachment to this letter *(Steps You Can Take to Further Protect Your Information)* for further information on steps you can take to protect your information.

Should you have any further questions please do not hesitate to contact a DEI Customer Service Representative at 1-800 430-5665.

Sincerely,
Manager, Dennis East International, LLC

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

COPY OF CREDIT REPORT

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

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

Experian
(888) 397-3742
www.experian.com
475 Anton Blvd.
Costa Mesa, CA 92626

TransUnion
(800) 916-8800
www.transunion.com
P.O. Box 1000
Chester, PA 19022

FRAUD ALERT

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information below:

Equifax
(888) 766-0008
www.alerts.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com/fraud
475 Anton Blvd.
Costa Mesa, CA 92626

TransUnion
(800) 680-7289
www.transunion.com
P.O. Box 2000
Chester, PA 19022-2000

Additional information is available at http://www.annualcreditreport.com.

SECURITY FREEZE

In some US states, including West Virginia, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $5.00 to place, lift or remove the security freeze.

To place a security freeze on your credit report, you need to send a request to a consumer reporting

agency by certified mail, overnight mail or regular stamped mail.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (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 fee of up to $5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft to the consumer reporting agency.

ADDITIONAL FREE RESOURCES ON IDENTITY THEFT

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.

Information for residents of California, Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, West Virginia, and Wyoming

It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing your credit card account statements and monitoring your credit reports closely for unauthorized activity.

Information for Iowa Residents

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

Information for Oregon Residents

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

Information for Residents of Illinois, Maryland and North Carolina

You can obtain information from the Federal Trade Commission about steps you can take to avoid identity theft, including how to place a fraud alert or security freeze. If you are a Maryland or North Carolina resident you may also be able to obtain this information from your State's Attorney General.

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or calling 410-576-6491].

MD Attorney General Office	**NC Attorney General's Office**	**Federal Trade Commission**
Consumer Protection Division	Consumer Protection Division	Consumer Response Center
200 St. Paul Place	9001 Mall Service Center	600 Pennsylvania Avenue, NW
Baltimore, MD 21202	Raleigh NC 27699-9001	Washington, DC 20580
1-888-743-0023	1-877-566-7226	1-877–IDTHEFT (438-4338)
www.oag.state.md.us	http://www.ncdoi.gov/	www.ftc.gov/bcp/edu/microsites/idtheft/