December 7, 2011

VIA CERTIFIED MAIL RETURN RECEIPT REQUESTED

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

Re: Legal Notice of Information Security Breach

Dear Sirs or Madams,

I write on behalf of Guide Publishing Group, Inc. and its affiliated website GuideYou.com (collectively, "GuideYou.com") to inform you of a potential information security breach that involved approximately 11 New Hampshire residents.

On October 28, 2011, GuideYou.com discovered that computer hackers may have unlawfully gained access to its server and customers' credit card information using malicious code. That same day, GuideYou.com contained the potential breach by removing the code.

GuideYou.com promptly self-reported the incident, by notifying its merchant bank, and engaged a computer forensic investigator to perform an investigation. The forensic investigator has reported that its investigation is 85% complete and has concluded that there was a cardholder data breach within the GuideYou.com environment.
The investigator believes that the initial compromise occurred on or about November 19, 2010. While GuideYou.com believes that data may not have been compromised until a much later date, as a courtesy it is notifying all customers who purchased from the GuideYou.com site between November 19, 2010 and October 28, 2011. The incident may have compromised customer cardholder data that may have included name, address, PAN, expiry, CVV2/CVC2/CID. GuideYou.com did not collect any Social Security numbers.

GuideYou.com is committed to safeguarding the privacy of personal information. GuideYou.com is cooperating diligently with the United States Secret Service as that agency seeks to identify and prosecute the perpetrator. GuideYou.com is deeply disappointed that this information may have been compromised and has already taken measures designed to prevent this from happening again in the future. In this instance, remediation efforts were made immediately on October 28, 2011, to secure the payment-processing environment.

GuideYou.com is notifying all affected individuals via written letter to each customer for whom GuideYou.com has sufficient contact information, and will post a notice to its website GuideYou.com/breach. These notifications will begin mailing and/or emailing on or before December 12, 2011. A copy of the form of notice being sent to impacted individuals is attached for your reference.

Sincerely,

Tanya L. Forsheit
Partner, InfoLawGroup LLP

Enclosure

GuideYou.com

Dear _____ ____:

On October 28, 2011, GuideYou.com discovered that computer hackers may have unlawfully gained access to our server and customers' credit card information using malicious code. That same day, GuideYou.com contained the potential breach by removing the code.

GuideYou.com promptly self-reported the incident, by notifying its merchant bank and engaged a computer forensic investigator to perform an investigation. The forensic investigator has reported that its investigation is 85% complete and has concluded that there was a cardholder data breach within the GuideYou.com environment

The investigator believes that the initial compromise occurred on or about November 19, 2010. We believe that data may have not been compromised until a much later date; however, as a courtesy, we are notifying all customers who purchased from our site between November 19, 2010 and October 28, 2011. The incident may have compromised your cardholder data that may have included your name, address, PAN, expiry, CVV2/CVC2/CID. We did not collect your Social Security number.

GuideYou.com is committed to safeguarding the privacy of personal information. We want you to be aware of this event. We are cooperating diligently with the United States Secret Service as that agency seeks to identify and prosecute the perpetrator. We recommend that you take a look at your account and see if there are any discrepancies and monitor your payment card statements and reports for unusual activity. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, call the bank that issued your credit or debit card immediately. We are deeply disappointed that this information may have been compromised and have already taken measures designed to prevent this from happening again in the future. In this instance, remediation efforts were made immediately on October 28, 2011, to secure the payment-processing environment.

Please review the attached "Information about Identity Theft Protection" for steps you may wish to consider taking to monitor your credit file and to protect yourself.

You can also obtain more information and assistance on our website, www.GuideYou.com/breach, or by calling toll-free (800) 690-0222.

Sincerely,

Drew Patterson

Drew Patterson

Enclosure

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790
800-685-1111	888-397-3742	800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC").

You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft.

> Federal Trade Commission, Consumer Response Center
> 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338),
> www.ftc.gov/idtheft
>
> For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: 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
>
> For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division
> 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity

theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below:

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
877-478-7625
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
Fraud Victim Assistance
Division
P.O. Box 6790
Fullerton, CA 92834-6790
800-680-7289
www.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Equifax

P.O. Box 105788
Atlanta, GA 30348
www.equifax.com

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

TransUnion
Fraud Victim Assistance
Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.