Nelson Mullins

Nelson Mullins Riley & Scarborough LLP
Attorneys and Counselors at Law
Atlantic Station / 201 17th Street, NW / Suite 1700 / Atlanta, GA 30363
Tel: 404 322.6000 Fax: 404.322.6033
www.nelsonmullins.com

Jon Neiditz
[redacted]

July 6, 2009

VIA CERTIFIED MAIL – RETURN RECEIPT REQUESTED

Attorney General Kelly A. Ayotte
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Breach at Nashbar Direct, Inc.

Dear Attorney General Ayotte:

We write to inform you of a recent data security incident on behalf of our client, Nashbar Direct, Inc. ("Nashbar"). Nashbar's previous website servers were recently the subject of an illegal attack that allowed unknown persons to obtain sensitive information of some of its customers even though such information was encrypted. Nashbar has determined that the breach may have disclosed the names, addresses, email addresses, web account password, and credit or debit card information of 1,307 residents in your state.

When Nashbar first learned of irregularities in its customers' credit or debit card statements, and before it was able to confirm that there was a problem, Nashbar took its website off-line, and then moved the website to an entirely new hosting environment and platform. Although its prior hosting company informed Nashbar that it could find no evidence of a breach, Nashbar engaged an outside, nationally recognized security firm to determine if, when and how the incident occurred and to confirm that the information Nashbar collects in its new hosting environment is protected to the fullest extent reasonably possible. Nashbar also reported this incident to Visa, MasterCard, American Express, Discover and the federal law enforcement authorities, with whom Nashbar is working to investigate this matter. Nashbar has received a few customer complaints describing unauthorized charges on their credit cards following the unauthorized access.

Simultaneously with this letter, our client is providing written notification to the affected residents in New Hampshire to the last home address our client has on record, and a sample of our notification letter is also enclosed. Although there is no evidence of misuse of the data to date, Nashbar has offered each affected customer a 30% discount on all purchases made on its new www.nashbar.com website for sixty (60) days.

Please do not hesitate to contact me at [redacted] if you have any questions.

Very truly yours,

Jon Neiditz

JAN:pb
Enclosures

bike nashbar.com

6103 State Route 446
Canfield, OH 44406

July __, 2009

VIA FIRST CLASS MAIL

<First Name><Middle Initial><Last Name><Suffix>
<Address> (Line 1)
<Address> (Line 2)
<City><State><Zip>

Dear <First Name><Middle Initial><Last Name><Suffix>,

Nashbar Direct, Inc. ("Nashbar") takes the privacy of its customers very seriously. We regret to inform you that our previous website servers were recently the subject of an illegal attack that allowed unknown persons to obtain the names, addresses, email addresses, web account password, and credit or debit card information of some of our valued customers, even though such information was encrypted. While the attack was confirmed on May 18, 2009, it appears that the unauthorized access began in December 2008. We began receiving a small number of customer complaints about unauthorized charges in mid-February 2009. We shut down the compromised website environment on March 3, 2009 and since then, our website has been in a new hosting environment and we have implemented additional security measures to further prevent unauthorized access to our customer information.

Even though we do not know if your information has been misused, we want to notify you of this incident, inform you of the steps Nashbar has taken to protect you against potential misuse of your credit or debit card information and provide direction to you on how to protect yourself against unauthorized charges to your credit or debit card or identity theft in general. We have been in business for 37 years, and this is the first incident of this nature to occur. We are determined to do everything we can to make sure it is the last.

Because we do not collect your Social Security number or other financial account information, the attacker only had access to the information described above. This should not subject you to risk of identity fraud or theft. No other information was potentially compromised. Although our prior hosting company informed us that it could find no evidence of a breach, we engaged an outside, nationally recognized security firm to determine if, when and how the incident occurred and to confirm that the information we collect in our new hosting environment is protected to the fullest extent reasonably possible. We also reported this incident to Visa, MasterCard, American Express, Discover and the federal law enforcement authorities, with whom we are working to investigate this matter.

To protect yourself from the possibility of unauthorized charges, and in the event your credit card issuer has not already contacted you or issued a new card, we recommend that ***you contact your credit card issuer immediately by calling the toll-free number located on the back of your card or on your monthly statement and request further guidance.*** You should tell your credit card issuer that your account may have been compromised and review all charges on your account for potentially fraudulent activity. We also recommend that you change your web account password immediately.

Although the attackers in this incident did not obtain enough personal information to affect your credit beyond possibly using the credit or debit card (again, you should contact your credit or debit card issuer if fraudulent charges have been made), there are some simple steps you can take to protect your financial identity more generally. First, you can always review your credit card bills, account statements and credit reports for unauthorized activity. You should also promptly report any suspected identity theft or fraud to your local law enforcement agency, the U.S. Federal Trade Commission, your financial institution and to the Fraud Alert phone line of one of the three national consumer reporting agencies by calling:

Experian:	1-888-397-3742
Equifax:	1-800-525-6285
TransUnion:	1-800-680-7289

You may obtain a 90-day Fraud Alert status on your credit record by calling one of the credit reporting agencies above. You also have the right to place a security freeze on your consumer report.

Also, under federal law, you are entitled to one free copy of your consumer credit report annually from each of the three national consumer reporting agencies. You may request your free annual consumer credit report by visiting www.annualcreditreport.com or by calling 1-877-FACTACT (1-877-322-8228). You may want to obtain copies of your consumer credit report to ensure the accuracy of the report information.

To learn more, you can contact the Federal Trade Commission ("FTC") at www.consumer.gov/idtheft, www.ftc.gov/credit or call 1-877-IDTHEFT (1-877-438-4338). You can also consult the New Hampshire Attorney General's Identity Theft Toolkit at http://doj.nh.gov/consumer/protection_kit.html.

To further assist you, we have also included a document that has answers to many of the questions you may have about this incident (see attached). If you have further questions about this incident, please call us at 1-800-999-1224 between 9 am and 5 pm (Eastern Standard Time), Monday through Friday (excluding holidays).

We value you as our customer. We appreciate the trust you place in us and would like to **offer you a 30% discount on your next purchase made before 8/28/2009**. Please make use of this discount by using the promotional code _____ along **with your customer number <Customer#>**. You may call our toll-free number at **1-800-NASHBAR**, or place an order at www.nashbar.com. For online orders, please be sure to login using the **customer number** printed on this letter. If you have a customer number but have never created an online account (and have previously used guest checkout), click on the "My Account" button, then the "Forgot Password" link. Enter your customer number, click on "Submit" and a password will be e-mailed to the e-mail address we have on file. Please login prior to adding items to your cart. The promotional code needs to be entered at the beginning of checkout. If you have any questions or experience any difficulties, please contact customer service at: **1-800-NASHBAR.**

Lastly, we've shared your passion for cycling for the past 37 years and remain committed to providing the best value and customer service available. We sincerely apologize for any inconvenience this event may have caused you.

Sincerely,

Jim Thompson
CEO
Nashbar Direct, Inc.

Responses to Your Questions

1. What personal information was accessed?

Your name, address, email address, web account password and credit card or debit card information. No Social Security numbers or dates of birth were involved.

2. What did you do when you discovered the breach?

We first asked our former outside vendor to conduct an investigation to determine whether there had been unauthorized access to our customer information. In the meantime, we shut down the compromised environment and moved our website to a new environment and platform. We then engaged outside experts to review our systems in order to determine whether a breach had occurred and what information had been taken. We also have implemented measures to further secure our systems based on the recommendations of outside experts.

3. Were other individuals affected or am I the only one?

Yes, other individuals were impacted by this incident. We are in the process of sending out notices similar to what you have seen today.

4. Should I be concerned about identity theft?

This is the first incident of this nature for us, but it is our understanding that the breach of credit card information happens frequently, and does not lead to identity theft when not associated with certain other personal information such as Social Security numbers or birth dates (that were not stolen here). Therefore, we do not believe there is a significant risk of identity theft arising from this incident. We do, however, suggest that you follow the suggestions in the letter that we sent to you, some of which are for your general protection rather than just in connection with this incident.

5. What should I do if I suspect fraudulent charges have been made on my credit or debit card?

We recommend that you immediately contact your credit or debit card issuer and let them know about the suspected fraudulent charges. Many issuers have toll-free numbers and 24-hour service to deal with such emergencies. You should be able to find the toll-free number on your card or on your statement. By law, once you report the loss or theft, you have no further responsibility for unauthorized charges. In any event, your maximum liability under federal law is $50 per card.

6. Do I need to contact Nashbar regarding this communication with an update of my status?

You do not need to update Nashbar on any further issues. Contact can be made if you have additional questions that are not covered here.