

**North Carolina Security Breach Reporting Form  
Pursuant to the Identity Theft Protection Act of 2005**

Name of Business Owning or Licensing Information Affected by the Breach: Digital Marketing Services, Inc. ("DMSI")  
Address: 2245 South Michigan Avenue  
Chicago, IL 60616  
Telephone: 312-328-7412  
Fax: 312-791-9660  
Email: dmlqrom@dmserv.com

**PLEASE SUBMIT FORM TO:**  
Consumer Protection Division  
NC Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
Telephone: (919) 716-6000  
Toll Free in NC: (877) 566-7226  
FAX: (919) 716-6050

Date Security Breach Reporting Form submitted: July 28, 2008  
Date the Security Breach was discovered: December 19, 2007  
Estimated number of affected individuals: Approximately 52,000 individuals were impacted.  
Estimated number of NC residents affected: Approximately 1,442 North Carolina residents were impacted.

Name of business maintaining or possessing information that was the subject of the Security Breach, if the business that experienced the Security Breach is not the same entity as the business reporting the Security Breach (pursuant to N.C.G.S. § 75-65(b)): Same as above.

Describe the circumstances surrounding the Security Breach and state whether the information breached was in electronic or paper format: Hackers accessed DMSI computers that potentially contained customers' information in electronic format by means of an SQL injection. Upon learning of the hacker attack, (continued on next page - A)

Regarding electronic information breached, state whether the information breached or potentially breached was password protected or encrypted in some manner. Yes If so, please describe the security measures protecting the information: The database was password protected and the server upon which the database resided was password protected, but the database was not encrypted. At the time of the attack, DMSI (continued on next page - B)

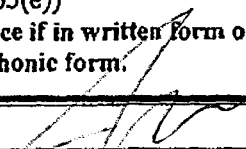
Describe any measures taken to prevent a similar Security Breach from occurring in the future: DMSI has implemented even tighter security to prevent this type of attack from occurring again.

Date affected NC residents were/will be notified: All NC residents were notified during the week of July 7, 2008.

If there has been any delay in notifying affected NC residents, describe the circumstances surrounding the delay pursuant to N.C.G.S. § 75-65(a) and (c): \_\_\_\_\_

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. § 75-65(c), please include the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. § 75-65(e))  
Please attach copy of the notice if in written form or a copy of any scripted notice if in telephonic form.  
 written notice  
 electronic notice (email)  
 telephone notice  
 substitute notice

Signature:  Date: 8/1/8  
Contact Person, Title: Ian C. Ballon, Shareholder  
Address: Greenberg Traub, LLP  
(if different from above) 2450 Colorado Ave., Suite 400E, Santa Monica, CA 90404  
Telephone: 310-586-6575 Fax: 310-586-0575 Email: balloni@gtlaw.com

Dear Valued Customer:

Although you may have already been contacted about this matter by your credit card issuer, we are writing to notify you that Direct Marketing Services, Inc. (DMSI) was the victim of a security breach. As a result, your credit card information on file with us, name and address may have been accessed by hackers between approximately October 9, 2007 and December 28, 2007. Upon learning of this hacker attack, we promptly commissioned a forensic audit as prescribed by VISA and industry best practices. We provided our merchant bank with a complete list of all potentially compromised accounts and we were advised that substantially all of the customer accounts in question had been protected, including in some cases by cancelling and reissuing new credit cards. We also have implemented even tighter security to prevent this type of attack from occurring again. We do not know whether your personal information in fact has been misused; however, we want to make you aware of some steps that we have taken to help you and give you suggestions on how to protect yourself. As a token of our appreciation for your continued patronage, we are also enclosing a 20% discount code that you may use on your next purchase from us at **[insert website(s)]**.

Rest assured that the only information that could have been obtained is the information listed above. No other information could have been accessed. In addition, under federal law, your liability for any fraudulent charges on a credit card account generally is limited to only \$50. As a precaution, we nonetheless recommend that if your credit card issuer did not cancel and reissue the credit card(s) you have on file with us, you: (1) require your credit card issuer to cancel and issue you a new card (some of the major credit card issuers offer overnight replacement if you ask for it) for each credit card account that you used to purchase goods from us in or before January 2008; and (2) closely review your credit card statements for those accounts and report to your credit card issuer any fraudulent charges.

There are also additional steps that you may take to protect yourself, which are outlined in the attached document.

In addition, we have engaged ConsumerInfo.com, Inc., an Experian® company, to provide you with one full year of credit monitoring, at no cost to you. This credit monitoring product known as Triple Alert<sup>SM</sup> will identify and notify you of key changes that are detected on any of your credit reports from the three credit reporting companies: Experian, Equifax® and TransUnion®. This credit monitoring product is a powerful tool that you can use to help you identify possible fraudulent use of your information.

Your complimentary 12-month Triple Alert membership includes:

- Daily monitoring of your three credit reports from Experian, Equifax and TransUnion
- Email alerts if key changes are detected on any of your three credit reports
- Monthly "No Hit" alerts, if applicable
- Toll-free access to a dedicated team of Fraud Resolution Representatives if you should detect any fraudulent activity or become a victim of identity fraud

- \$10,000 in identity theft insurance provided by Virginia Surety Company, Inc. with no deductible\*

\*Due to New York state law restrictions, identity theft insurance coverage cannot be offered to residents of New York.

You have until October 8, 2008, to activate this membership, which will then continue for 12 full months. We encourage you to activate your credit monitoring membership as soon as possible.

To sign up, please visit <http://partner.consumerinfo.com/dmsi> and enter your individual activation code provided below. Please keep in mind that once activated the code cannot be re-used. You will be instructed on how to enroll in your complimentary credit monitoring product. All credit reports and alerts will be delivered via email.

Your Single Use Credit Monitoring Activation Code: **[insert Activation code]**

We recognize that this incident may be upsetting and may have inconvenienced you. Accordingly, as a token of our appreciation for your continued patronage, we are providing you with a 20% discount code that you may use on your next purchase from us. In order to claim this discount, use the following code: **[insert CODE]**. We are also enclosing a general information sheet on additional steps you may take to protect yourself against the threat of identity theft.

If you have any further questions, please do not hesitate to contact us by telephone at 1-800-227-7598 or by writing to Customer Service, P.O. Box 2789, Cedar Rapids, IA 52406-2789.

Sincerely,

## Steps Consumers Should Take To Combat Identity Theft

- Remain vigilant over the next 12 months and review your credit card bills and credit report for unauthorized activity.
- Promptly report any suspected identity theft or fraud to your local law enforcement agency, the U.S. Federal Trade Commission and your state attorney general. You can call the U.S. Federal Trade Commission at 1-877-ID-THEFT (1-877-438-4338), visit the website at <https://www.ftccomplaintassistant.gov/> or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580. The following website lists the names, telephone numbers and addresses of the state attorney generals: [http://www.naag.org/ag/full\\_ag\\_table.php](http://www.naag.org/ag/full_ag_table.php). You can also obtain additional information from these sources about additional steps you can take to avoid identity theft.
- Promptly report any suspected identity theft or fraud to your financial institution, and to the Fraud Alert phone line of one of the three national consumer reporting companies by calling: Experian 1-888-397-3742; Equifax 1-800-525-6285; or TransUnion 1-800-680-7289.
- Contact the fraud departments of the three national consumer reporting companies to discuss your options, including obtaining a 90 day Fraud Alert status on your record.
- If you are the victim of identity theft, as a result of this incident or otherwise, promptly file a police report with the police in your area. You have the right to obtain a copy of this police report relating to your identity theft. You may also wish to contact your credit card issuers and financial institutions and inform them of the incident as well.
- Place a security freeze on your consumer report. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent; however, please be aware that using a security freeze may delay your ability to obtain credit. You may request that a security freeze be placed on your consumer report by sending a request to a consumer reporting company by certified mail, overnight mail or regular stamped mail to the addresses below. The following information should be included when requesting a security freeze: (a) name; (b) address; (c) date of birth; (d) social security number; (e) proof of current address such as a current utility bill; and (f) payment of applicable fees to request a security freeze of your credit file. Please note that there are certain fees that may be associated with placing a security freeze on your consumer report. Most agencies accept personal checks, American Express, Mastercard, VISA, and Discover Cards for payment of fees. Please call each Credit Agency at the numbers provided below to determine the fee for your state and what forms of payment are accepted. If you are paying by credit card, please include the following information: (a) name of the person as it appears on the credit card; (b) type of credit card (American Express, Mastercard, VISA, or Discover Card); (c) complete account number; (d) expiration data (month and year); (e) for American Express - 4 digit Card Identification Number (on front of card above the account number); and (f) for Mastercard, VISA, or Discover Card - 3 digit Card Identification Number (on back of card at the end of the account number. Please do not send cash through the mail. Additional information may be obtained by calling Equifax at 1-800-525-6285, TransUnion at 1-800-680-7289 and Experian at 1-888-397-3742 or by going to the following websites: Equifax (<http://www.equifax.com>), TransUnion (<http://www.transunion.com>) and Experian (<http://www.experian.com>). In addition, if you have been a victim of identity theft, you must file and include with your request a copy of a police report, identity theft report, or other government or law enforcement agency report, such as a DMV report.

Send your request for a security freeze to the following addresses:

(1) Equifax

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
1-888-766-0008

(2) TransUnion

TransUnion  
Fraud Victim Assistance Department  
P.O. Box 6790  
Fullerton, CA 92834  
1-800-680-7289

TransUnion  
Fraud Victim Assistance Department  
1561 E. Orangethorpe Ave.  
Fullerton, CA 92831

(Use this address only if you are a New York, New Jersey, and West Virginia resident who is making your request to TransUnion via overnight mail. All other individuals should make their request to the address above.)

(3) Experian

The address for Experian varies depending on your state of residence and the manner in which you send your request (e.g.: overnight mail, regular mail, certified mail, etc.). Please call Experian at 1-888-EXPERIAN (1-888-397-3742) or visit Experian's website at the following URL and select your state of residence to find the appropriate address: [http://www.experian.com/consumer/security\\_freeze.html](http://www.experian.com/consumer/security_freeze.html).

To find out more information about security freezes and each agency's particular requirements, visit the agency websites located at:

(1) Equifax

[http://www.equifax.com/cs/Satellite?c=EFX\\_ContentRoot&cid=1165203975981&pageName=5-1%2F5-1\\_Layout](http://www.equifax.com/cs/Satellite?c=EFX_ContentRoot&cid=1165203975981&pageName=5-1%2F5-1_Layout)

(2) TransUnion

<http://www.transunion.com/corporate/personal/fraudIdentityTheft/preventing/securityFreeze.page>

(3) Experian

[http://www.experian.com/consumer/security\\_freeze.html](http://www.experian.com/consumer/security_freeze.html).