KELLEY DRYE & WARREN LLP
A LIMITED LIABILITY PARTNERSHIP
WASHINGTON HARBOUR, SUITE 400
3050 K STREET, NW
WASHINGTON, D.C. 20007-5108
(202) 342-8400

NEW YORK, NY
LOS ANGELES, CA
CHICAGO, IL
STAMFORD, CT
PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICE
MUMBAI, INDIA

FACSIMILE
(202) 342-8451
www.kelleydrye.com

ALYSA Z. HUTNIK
DIRECT LINE: (202) 342-8603
EMAIL: ahutnik@kelleydrye.com

CHRISTOPHER M. LOEFFLER
DIRECT LINE: (202) 342-8429
EMAIL: cloeffler@kelleydrye.com

May 29, 2013

Office of the Attorney General
State of New Hampshire
33 Capitol Street
Concord, NH 03301
Attn: Security Breach Notification

Re: Information Security Incident Notification

To whom it may concern:

Pursuant to your state's law, Shumsky Promotional Agency is notifying your office of an information security incident that involves the personal information of approximately 1 New Hampshire resident. On May 16, 2013, Shumsky was notified by its e-commerce platform provider that on approximately May 14, 2013 an unauthorized third party accessed Shumsky's data system containing approximately 1,400 Shumsky records. The consumer personal information that may have been accessed includes cardholder name, address, email, credit / debit card number, expiration date, and CVV code.

Shumsky and its service providers have been diligently investigating the incident to determine its scope and apply proper remediation. On May 15, 2013 (the day after the breach), Shumsky's service providers identified the breach and immediately implemented security measures designed to stop the attack and prevent it from recurring. These measures included applying security patches to the relevant systems, and hiring experts to review and coordinate additional safeguards. Shumsky is also working with the payment card brands concerning the specific payment cards at issue in this incident.

Shumsky is providing direct notification to potentially affected consumers via both email with a link to additional steps a consumer can take to protect his or her information, and via letter sent by postal mail that encloses the additional steps to protect information, and is providing a toll-free telephone number that recipients may call for additional information and assistance.

Please find enclosed a copy of the written notice of the security incident sent to the New Hampshire resident. Please contact us with any questions or concerns.

Sincerely,

Alysa Z. Hutnik
Christopher M. Loeffler

Enclosure

Email SUBJECT: PLEASE READ: Message regarding your card ending in [last 4 digits]

Dear _____:

Re: Card ending in [last 4 digits of the compromised card]

On May 16, 2013, Shumsky was notified by its e-commerce platform provider that on May 14, 2013, an unauthorized third party accessed the e-commerce platform and accessed nearly 1,400 of Shumsky cardholder records. We understand our service provider patched the vulnerability the very next day, on May 15. We have engaged with proper security advisors and technical experts to rectify the situation however, as a result of the incident, we are writing to you to make you aware that your credit/debit card information might have been accessed by an unauthorized party. This information included your name, address, email, credit/debit card number, expiration date, and CVV code. Shumsky does NOT collect PINs for debit cards, SSNs, dates of birth or driver's license numbers thus this type of sensitive information was not involved.

Shumsky regrets this incident, has immediately engaged with technical and legal advisors to work through the situation, and put in place updated measures to prevent this from happening again. Shumsky is also working with the payment card brands concerning the specific payment cards at issue in this incident. Nevertheless, we recommend that you monitor your payment card account for potential unauthorized charges and alert your financial institution to monitor or potentially cancel and reissue you a new card as they determine is prudent.

If you have further questions, please contact Shumsky at 1-800-414-8946 or 937-221-7103 between 8am and 5pm EST.

Additionally, we have enclosed information on steps you can take to further protect your information. Please go to: http://www.shumsky.com/cardinfo.html to see the details.

Shumsky takes this matter very seriously and deeply regrets any inconvenience or concern that this matter may cause you.

Sincerely,

Anita Emoff

President
Shumsky, 811 E. 4th Street, Dayton OH 45402

[COMPANY Letterhead]

[Recipient Name]
[Recipient Address 1]
[Recipient Address 2]

[Date]

Dear _____:

Re: Card ending in [last 4 digits of the compromised card]

On May 16, 2013, Shumsky was notified by its e-commerce platform provider that on May 14, 2013, an unauthorized third party accessed the e-commerce platform and accessed nearly 1,400 of Shumsky cardholder records. We understand our service provider patched the vulnerability the very next day, on May 15. We have engaged with proper security advisors and technical experts to rectify the situation however, as a result of the incident, we are writing to you to make you aware that your credit/debit card information might have been accessed by an unauthorized party. This information included your name, address, email, credit/debit card number, expiration date, and CVV code. Shumsky does NOT collect PINs for debit cards, SSNs, dates of birth or driver's license numbers thus this type of sensitive information was not involved.

Shumsky regrets this incident, has immediately engaged with technical and legal advisors to work through the situation, and put in place updated measures to prevent this from happening again. Shumsky is also working with the payment card brands concerning the specific payment cards at issue in this incident. Nevertheless, we recommend that you monitor your payment card account for potential unauthorized charges and alert your financial institution to monitor or potentially cancel and reissue you a new card as they determine is prudent.

If you have further questions, please contact Shumsky at 1-800-414-8946 or 937-221-7103 between 8am and 5pm EST.

Additionally, we have enclosed information on steps you can take to further protect your information. You may also access http://www.shumsky.com/cardinfo.html for more details.

Shumsky takes this matter very seriously and deeply regrets any inconvenience or concern that this matter may cause you.

Sincerely,

Anita Emoff

President
Shumsky, 811 E. 4th Street, Dayton OH 45402

Steps You Can Take To Further Protect Your Information

- **Review Your Account Statements**

As a precautionary measure, we recommend that you review 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, or the Federal Trade Commission.

- **Credit Report Monitoring**

You may obtain a free copy of your credit report from each of the 3 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 http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies shown below.

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	TransUnion (800) 916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834

- **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). **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.state.md.us, or calling 410-576-6491. **North Carolina residents** may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov, by calling 8770566-7226, or writing to 9001 Mail Service Center, Raleigh, North Carolina 27699.

- **Fraud Alert**

You may consider placing a fraud alert on your credit report. This fraud alert statement 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 identified above. Additional information is available at http://www.annualcreditreport.com.

- **Security Freeze**

In some U.S. states, 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. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift, or remove the security freeze; however, this fee may be less in certain states (in MA, up to $5). In order to place a security free, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. You must separately place a security freeze on your credit file with each credit reporting agency.