VORYS

**Vorys, Sater, Seymour and Pease LLP**
Legal Counsel

**52 East Gay St.**
**PO Box 1008**
**Columbus, Ohio 43216-1008**

**614.464.6400 | www.vorys.com**

**Founded 1909**

**Eric S. Whisler**
**Direct Dial (614) 464-5691**
**Direct Fax (614) 719-4945**
**Email eswhisler@vorys.com**

May 31, 2013

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

Re: Notification of Security Breach

To whom it may concern:

On behalf of our client, Goldner Associates, Inc. ("Goldner Associates"), and pursuant to your state's law, we are writing to inform you of a recent security incident involving approximately 3 residents of your state. Goldner Associates, a family run business, provides e-commerce services to its customers to allow those customers to create online stores for company-branded products. Goldner Associates was advised on May 16, 2013 of possible unauthorized access to the server of its service provider hosting the online stores. On May 17, 2013, Goldner Associates' service provider confirmed that there was unauthorized access that occurred on May 14, 2013.

The consumer personal information that was accessed includes name, credit card or debit card number and the expiration date and CVV code for the card, and the address and phone number of individuals who had made purchases through one of the online stores. Since Goldner Associates does not collect PINs for debit cards, and does not collect social security numbers, dates of birth or driver's license information, these types of personal information were not involved. The credit card and debit card information was encrypted at the time of the unauthorized access, but based on a common point of purchase notice from a card brand, it appears the encryption key was also accessed.

Upon learning of the breach, Goldner Associates promptly worked with its service provider to implement several measures to address this unauthorized access. Those steps included determining how the unauthorized access was obtained and then shutting down that means of access. Goldner Associates also had its service provider remove all credit card data from the system and has implemented a tokenization system so it will no longer be necessary to retain payment card information. In addition, Goldner Associates immediately engaged outside

experts to assist in this situation. Finally, Goldner Associates is working with its payment card processor and card brands concerning the specific payment cards at issue in this incident.

Goldner Associates is providing direct notification in compliance with your state's law to affected consumers via letter sent by postal mail that includes information regarding additional steps a consumer can take to protect his or her information. The mailed notification is a follow up to an email notice sent to affected consumers on the same day the unauthorized access was confirmed, May 17, 2013. The email notification informed affected consumers of the unauthorized access and that they should monitor their payment card activity.

Please find enclosed a copy of both the email and letter notice prepared by Goldner Associates for residents of your state. Please contact us with any questions or concerns.

Very truly yours,

Eric S. Whisler

ESW/csp
Enclosures
cc: Mitch Emoff

**[Interim Email Notice]**

Goldner Associates, Inc., who provides services to **[Goldner customer name]**, was made aware on May 17 of unauthorized access to our online ordering system. This unauthorized access resulted in theft of credit card information. As a result of this breach we immediately changed our credit card policies and increased security on the **[Goldner customer name]** Company Store.

We believe your credit card ending in **[fill in last 4 digits]** was stolen. We are notifying you so you can monitor charges on this card. If you suspect unauthorized use of your credit card, you should immediately contact your credit card company to notify them of the possible unauthorized transactions.

We sincerely apologize for any inconvenience this causes. Please be assured that we are working with experts to fully address this issue and taking this very seriously.

**[Sample Consumer Notification Letter]**
**[Company Letterhead]**

**[Date]**
**[Name]**
**[Address]**
**[City, State ZIP]**

Dear **[Name]**,

Re: Card ending in **[last 4 digits of card affected]**

We recently notified you of the security incident involving the **[Goldner customer name]** online store. As we noted in the email that we sent to you, Goldner Associates provides services to **[Goldner customer name].** By way of update from our May 17th email, we have now confirmed that on May 14, 2013 there was unauthorized access to the server of our service provider hosting the **[Goldner customer name]** online store. We have also confirmed that these unauthorized third parties obtained your name, credit card or debit card number for the card noted above and the expiration date and CVV code of that card, and your address and phone number. Since we do not collect PINs for debit cards, social security numbers, dates of birth or driver's license information, these types of personal information were not involved.

We promptly worked with our service provider to implement several measures to address this unauthorized access. Those steps include working with our hosting company to determine how the hacker obtained access to the system and then shutting down that means of access. We have also removed all credit card data from the system. We are implementing a tokenization system so it will no longer be necessary to retain your credit card information. Finally, we immediately engaged outside experts to assist us in this situation and to put in place the noted measures.

We deeply regret this unfortunate situation. Even with the measures noted that we have taken, we recommend you to take preventative measures. We encourage you to vigilantly monitor your credit and debit card account statements. If the card that you used with us was a debit card, we suggest you contact your bank who issued your card and follow their recommendations. If you notice fraudulent charges on the card noted above, you should contact your card issuer.

While credit card fraud is generally not considered identity theft, we understand that you may want information on identity theft and detailed instructions on other actions you might consider. We have enclosed additional steps that you can take to further protect your information.

We sincerely apologize for any inconvenience that this may cause you. If you have additional questions, please call us toll-free at 1-800-213-4111, Monday through Friday, 8:00 AM to 5:00 PM central time.

Sincerely,

Goldner Assoicates, Inc.

## Further Information and Steps You Can Take

Information from the Federal Trade Commission

The Federal Trade Commission has gathered this information and provides its suggestions for actions in the event of identity theft at http://www.consumer.ftc.gov/features/feature-0014-identity-theft. You may also contact the Federal Trade Commission for more information toll-free at 1-877-ID-THEFT (438-4338) (TTY: 1-866-653-4261), or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Obtaining a free credit report or placing a security freeze

You may obtain a free copy of your credit report from each of the credit bureaus once a year by going to http://www.annualcreditreport.com online, or call toll free 877-322-8228. Hearing impaired consumers can access TDD service at 877-730-4104. You should monitor these reports. You may also place a security freeze on your credit report by contacting the credit bureaus as listed below.

| Equifax | Experian | TransUnion |
|---|---|---|
| 888-766-0008 | 888-397-3742 | 800-680-7289 |
| www.equifax.com | www.experian.com | www.transunion.com |

Filing a Police Report for Suspicious Activity

If you do find suspicious activity on the credit or debit card indicated in our notice to you or in your credit report, 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. In addition, you should report identity theft to your Attorney General and the Federal Trade Commission.