Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

August 16, 2018

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

RE: Notice of Data Security Incident

Dear Attorney General Gordon J. MacDonald,

We represent OMNIA Partners, Inc. ("OMNIA"), located at 840 Crescent Drive, Suite 600, Franklin, TN 37067 and are writing to notify your office of an incident that may affect the security of certain personal information relating to residents of your state. By providing this notice OMNIA does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about July 11, 2018, OMNIA discovered suspicious emails generated from an employee's email account. OMNIA immediately commenced an investigation and discovered that the organization was the victim of a recent phishing attack. This incident was focused on capturing credentials to employee email accounts in the cloud system used by OMNIA and its employees. Third party forensic investigators were retained to assist with determining the nature and scope of the impact of this incident on the organization. The investigation determined that one employee email account was accessed without authorization between May 21, 2018 and July 11, 2018. Credentials for this email account were changed to prevent further unauthorized access. A review of the contents of the email account was undertaken to identify what information may have been accessible and who may be affected. On or about August 7, 2018, it was determined that certain information related to certain individuals was included in emails that may have been viewed without authorization.

The information that may have been subject to unauthorized access includes name and social security number.

Notice to New Hampshire Resident

On or about August 16, 2018, OMNIA began providing written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, OMNIA moved quickly to investigate and respond to the incident, assess the security of OMNIA systems, and notify potentially affected individuals and applicable regulators. OMNIA is also working to implement additional safeguards and training to its employees.

OMNIA is providing free access to one year of credit monitoring and fraud resolution services through Experian to individuals whose information was accessible in the email account. Additionally, OMNIA is providing guidance on how to protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. OMNIA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/alc
Enclosure

EXHIBIT A

OMNIA
PARTNERS

August 16, 2018

{First Name} {Last Name}
{Address}
{City}, {State} {Zip}

Re: Notice of Data Breach

Dear {First Name} {Last Name},

We write to inform you of a data privacy incident that may involve certain information related to you. We take this incident very seriously and are providing you with information and access to resources so that you can better protect your personal information, should you feel it is appropriate to do so.

What Happened? On or about July 11, 2018, we discovered suspicious emails generated from an employee's email account. OMNIA Partners, Inc. ("OMNIA") immediately commenced an investigation and discovered that the organization was the victim of a recent phishing attack. This incident was focused on capturing credentials to employee email accounts in the cloud system used by OMNIA and its employees. Third party forensic investigators were retained to assist with determining the nature and scope of the impact of this incident on our organization. The investigation determined that one employee email account were accessed without authorization between May 21, 2018 and July 11, 2018. Credentials for this email account have been changed to prevent further unauthorized access. A review of the contents of the email account was undertaken to identify what information may have been accessible and who may be affected. On or about August 7, 2018, it was determined that certain information related to you was included in emails that may have been viewed without authorization.

What Information Was Involved? The information related to you that was identified during the review of the emails that may have been viewed includes your name and Social Security number.

What We Are Doing. We have security measures in place to protect the data in our care and have taken additional measures as a result of this incident, including providing additional training to employees on how to spot and respond to suspected phishing attacks and introducing additional authentication measures to the cloud system. We are reporting this incident to applicable state regulators as well as to the individuals who may be affected by this incident. We are also providing you with information about this event and about the steps you can take to help protect against misuse of your personal information, should you feel it appropriate to do so.

Out of an abundance of precaution, we are offering you access to one year of membership of Experian's® IdentityWorks℠ at no cost to you. The cost of this service will be paid for by us. This product provides you with superior identity detection and resolution of identity theft. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information." You can also enroll to receive the free credit monitoring and identity theft protection services we are offering.

To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **November 30, 2018** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.890.9332 by

November 30, 2018. Be prepared to provide engagement number as proof of eligibility for the identity restoration services by Experian.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call Skip Jones at 615-786-1156 between 8 a.m. and 5 p.m. Central time, Monday through Friday, excluding major U.S. holidays. We take the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Skip Jones
Chief Information Officer

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.890.9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your personal account statements and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. Contact information for the credit reporting agencies can be found below.

Fraud Alerts. At no charge, you can also have the three major credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/	freeze.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General, as well as the credit reporting agencies listed above. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. You have the right to file a police report if you ever experience identity theft or fraud, and instances of known or suspected identity theft should be reported to law enforcement. Please note that in order to file a police report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. This notice has not been delayed as the result of a law enforcement investigation.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions