Troutman Pepper Hamilton Sanders LLP
301 Carnegie Center, Suite 400
Princeton, NJ 08540-6227

troutman.com

Angelo A. Stio III
angelo.stio@troutman.com
609-951-4125

May 3, 2021

VIA EMAIL
doj-cpb@doj.nh.gov

John Formella, Esq.
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General Formella:

This firm represents OHL North America ("OHL") which is located at 26-15 Ulmer Street, College Point, NY 11354, and is a construction company specializing in large public works projects. We are writing, pursuant to N.H. Rev. Stat. § 359-C:19 *et seq.* to notify you of an incident that may affect the security of personal information related to five (5) New Hampshire residents.

During the week of March 14, 2021, OHL discovered that a third party accessed its environment (the "Incident") and was attempting to encrypt files. Upon discovering the unauthorized access, OHL was able to quickly prevent the encryption from occurring, remove the third party from its environment and secure its systems. Thereafter, OHL commenced an investigation with the assistance of a third party consultant to, among other things, determine the cause of the Incident, confirm the third party was expelled from its systems and to determine if any files were accessed.

On April 13, 2021, OHL discovered that the third party had exfiltrated certain employee files from its system. The employee files that were accessed included payroll records, and information on OHL's employee benefits plan. The information in these files included names, addresses, email addresses, phone numbers, dates of birth, part or all of social security numbers and certain bank account information, but not any passwords or access codes. OHL reported the incident to law enforcement and OHL's investigation of the Incident is on-going. OHL will update you if any additional information is uncovered.

Beginning on May 4, 2021, OHL will mail written notice of the Incident to all employees that may be affected, including the five (5) New Hampshire residents referenced above. OHL has arranged for all affected employees to receive a twenty-four (24) month membership in Experian's IdentityWorksSM credit monitoring and identity theft protection at no cost. Experian's

IdentityWorksSM provides credit monitoring services, identity theft fraud alerts and up to $1 million in identity fraud insurance (with $0 deductible). A copy of the sample notice is attached hereto as **Exhibit A.** Notification to New Hampshire residents has not been delayed by the Federal Bureau of Investigation's involvement.

Please note that by providing this notice, OHL does not waive any rights or defenses, including but not limited to, defenses related to the applicability of New Hampshire law and personal jurisdiction. If you have any questions or require any additional information regarding this Incident, please do not hesitate to contact me.

Sincerely,

/s/ Angelo A. Stio III

Angelo A. Stio III

AAS/MRC
Enclosure

[OHL LETTERHEAD]

May 4, 2021

[Recipient]

NOTICE OF BREACH

OHL North America ("OHL") is committed to protecting the privacy of its employees and their family members. As part of this commitment, we are writing to advise you of an incident (the "Incident") that may involve unauthorized access to some of your personal information. Set forth below is information concerning the Incident along with some resources that can help you protect against the possibility of misuse of your information, if you choose to employ them.

What Happened?

During the week of March 14, 2021, OHL discovered that a third party accessed its system. Upon discovering the unauthorized access, OHL was able to quickly remove the third party from its environment and secure its systems. Thereafter, OHL commenced an investigation with the assistance of a third party consultant to, among other things, determine the cause of the Incident, confirm the third party was expelled from its systems and to determine if any files were accessed and exfiltrated. Based on the investigation, the third party consultant believes the data breach may have occurred between March 18, 2021 and April 8, 2021. On April 13, 2021, OHL first learned that the third party had accessed and exfiltrated files.

What Information Was Involved?

We believe the employee files that were accessed included payroll records, and information on OHL's employee benefits plan. These files included, among other things, your name, address, phone number, email address, date of birth, part or all of your social security number and certain bank account information, **but not** any passwords or access codes. OHL has reported the incident to law enforcement and its investigation of the Incident is on-going. OHL will update you if there are any material developments for your personal data.

What We Are Doing?

OHL is reviewing its security measures and working to implement additional safeguards to reduce the risk of similar incidents occurring in the future.

In addition, OHL has arranged and is paying for you to receive a twenty four (24) month membership of Experian's IdentityWorksSM credit monitoring and identity theft protection. Depending on which jurisdiction you live in, the membership may also include $1 million identity theft insurance. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: 8/31/2021 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bplus
- Provide your activation code that is listed at the top of this letter below your name and answer all questions
- Engagement # _____ will be needed for online or phone registration

If you have questions about the product or would like to enroll over the phone, please contact Experian's customer care team at 877-890-9332 by 8/31/2021.

What You Can Do?

Outlined below are a number of ways that you can protect yourself.

a. *Remain Vigilant*

We recommend that you remain vigilant by reviewing your financial account statements and credit reports.

b. *Obtain Your Credit Report*

You can obtain a free copy of your credit report from each of the three national credit reporting agencies once every 12 months by visiting 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 also can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies directly. Contact information for the three national credit reporting agencies is provided below:

Equifax	Experian	TransUnion
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

c. *Notify Law Enforcement of Suspicious Activity*

If you detect suspicious activity on any account, you should promptly notify the financial institution or company with which the account is maintained and report any suspected incidents of identity theft to local law enforcement authorities or your state attorney general. To report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft you can go to the FTC's Web site, at www.consumer.gov/idtheft, or call the FTC at (877) IDTHEFT (438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You also have the right to file or obtain a police report if you experience identity theft. 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 proof that you have been a victim. A police report is often required to dispute fraudulent items.

d. *Place a Fraud Alert or Security Freeze on Your Credit Report File*

You also may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three national consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
(800) 349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
(888) 397-3742

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
(888) 909-8872

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a mechanism to enable you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

To remove a security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests

made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

e. *Additional Information on how to protect your identity.*

You can also further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the credit reporting agencies, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438-4338); and TTY: 866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can also obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For District of Columbia Residents: For additional information about steps to take to avoid identity theft, you may contact the District of Columbia Attorney General at 441 4th Street, NW, Washington, DC 20001, (202) 727-3400, dc.oag@dc.gov. Additionally, you may also contact the Office of Consumer Protection at Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001, (202) 442-9828, consumer.protection@dc.gov.

For Maryland Residents: Visit the state Attorney General's Web site at www.marylandattorneygeneral.gov/Pages/IdentityTheft, or call the Maryland Attorney General's Identity Theft Unit at (410) 576-6491, or send an email to idtheft@oag.state.md.us, or write to Maryland Attorney General, Identity Theft Unit 200 St. Paul Place, 25th Floor, Baltimore, MD 21202 to report incidents of identity theft or for additional information.

For Massachusetts Residents: In addition to the above steps, under Massachusetts law, you have a right to obtain a police report with regard to the Incident. In addition, if you are the victim of identity theft, you have a right to file a police report and obtain a copy of it.

For North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the sight to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for

credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting http://www. https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York Residents: The Attorney General can be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755. For additional information, you can also visit the Attorney General's Web site at www.ag.ny.gov, call the New York Attorney General's Bureau of Internet and Technology (BIT) at (212) 416-8433, send an email to ifraud@ag.ny.gov, or write to New York Attorney General, Bureau of Internet and Technology, 28 Liberty Street, New York, NY 10005. You may also go to the New York Department of State, Division of Consumer Protection's Web site at www.dos.ny.gov/consumerprotection/identity_theft/index.htm, or call the Consumer Helpline at (800) 697-1220 to report incidents of identity theft or for additional information.

For Oregon Residents: In addition to notifying the Federal Trade Commission as detailed above, you may report suspected identity theft to law enforcement, including the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392 (toll-free in Oregon), (503) 378-4400, http://www.doj.state.or.us.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.

- **More Information**

We sincerely regret any inconvenience or concern that this Incident may cause you. Please let us know promptly if you discover any suspicious activity or if you have any questions or concerns. Please contact Abby Reich at 718-554-2375 or abby.reich@ohlna.com

Sincerely,

Abby Reich