MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

July 13, 2018

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 033301

Re: Notice of Data Event

Dear Mr. MacDonald:

We represent Roadrunner Transportation Systems, Inc. ("RRTS"), 4900 South Pennsylvania Ave., Cudahy, WI 53110, and are writing to notify your office of an incident that may affect the security of personal information relating to three (3) New Hampshire residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, RRTS does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On June 22, 2018 it was determined through a forensic investigation that an unauthorized actor used a phishing email campaign to gain access to certain employees' email accounts at RRTS. Through the investigation, we determined that in addition to the email account access, the actor(s) also gained access to our human resources platform, Workday. The access to these accounts occurred between May 16, 2018 through May 27, 2018. Additionally, the investigation determined that the Workday accounts may have been viewed without authorization.

Notice to New Hampshire Residents

RRTS provided written notice to potentially affected individuals by mail on or about July 13, 2018, which includes three (3) New Hampshire residents. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and to Be Taken

Upon discovering the incident, RRTS moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident.

RRTS is providing all potentially affected individuals complimentary access to twelve (12) free months of credit and identity monitoring services, including identity restoration services, through AllClear. Additionally, RRTS is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. RRTS is also providing written notice of this incident to the F.B.I. and other state regulators as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4798.

Very truly yours,

James E. Prendergast of
MULLEN COUGHLIN LLC

JEP/rab
Enclosure

Exhibit A

Logo/Letterhead for RRTS

[Name]
[Address1]
[Address2]
[City, State Zip]

July 13, 2018

Re: Notice of Data Security Incident

Dear [Name of Affected Individual]:

We write regarding a recent email phishing event that may have impacted the security of your personal information. We want to provide you with information about the incident, our response and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

What Happened? On May 30, 2018, Roadrunner Transportation Systems, Inc. ("RRTS") became aware that they were the subject of a phishing campaign attack and that several employees had inadvertently clicked on the phishing email. RRTS immediately commenced an investigation into this activity to determine what happened and what information may be affected. This investigation included working with third party forensic investigators to confirm the nature and scope of this incident. Through the investigation, we determined that there was unauthorized access to several employee email accounts as well as Workday accounts between May 16, 2018 through May 27, 2018. It is believed that this access occurred after the employees received phishing emails. Further investigation determined that the unauthorized user then gained access into the Workday accounts utilizing information obtained from the phishing campaign. Ultimately, some direct deposit accounts were changed by the attacker. However, RRTS discovered the intrusion before any funds were transferred.

What Information was Involved? A review of the Workday accounts determined that information related to you was contained therein that may have been viewed without authorization. This information included your name, address, social security number, phone number, date of birth, payroll information, dependent information and health plan information.

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. Upon learning of the event, we immediately commenced an investigation to confirm the nature and scope of the incident and to identify what information may be affected. We also took steps to prevent further unauthorized access to the email accounts and Workday accounts by changing passwords. While we have measures in place to protect information in our systems, we are reviewing our existing policies and procedures.

As an added precaution, we are offering you access to twelve months (12) of credit monitoring and identity theft restoration services through AllClear at no cost to you. Please review the attached "Steps You Can Take to Protect Your Information" for information on these services and instruction on how to enroll. We encourage you to enroll in these services as we are not able to act on your behalf to do so.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information," which contains information on what you can do to better protect against possible misuse of your information. You may also enroll in the credit monitoring and identity theft restoration services we are offering. In addition, we encourage you to routinely change your passwords to your accounts to avoid unauthorized access.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please contact Robert M. Milane, General Counsel & Chief Compliance Officer, at bmilane@rrts.com or (414) 486-8448.

Sincerely,

Robert M. Milane
General Counsel & Chief Compliance Officer

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll Credit Monitoring

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-877-676-0379 using the following redemption code: {RedemptionCode}.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may be required in order to activate your monitoring options

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports and explanation of benefits forms for suspicious activity. 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 listed below to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these 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	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19106
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	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 P.O. Box 105788 Atlanta, GA 30348 1-800-685-1111 www.freeze.equifax.com	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/	TransUnion P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com/credit-freeze

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. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice was not delayed as the result of a law enforcement investigation.