UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

GEORGE NELSON, on behalf of himself and all others similarly situated, Plaintiff, v. ROADRUNNER TRANSPORTATION SYSTEMS, INC., Defendant.	)	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff George Nelson ("**Plaintiff**"), individually and on behalf of all others similarly situated, by and through counsel, brings this action against Defendant Roadrunner Transportation Systems, Inc. ("**Defendant**" or "**Roadrunner**"), and alleges as follows based upon personal knowledge, investigation of counsel, and information and belief:

PARTIES

1. Plaintiff George Nelson is a citizen and resident of Greensburg, Kentucky.

2. Defendant Roadrunner Transportation Systems, Inc. is a resident of Illinois.

JURISDICTION AND VENUE

3. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act 28 U.S.C. § 1332(d) ("**CAFA**"), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 Class Members, and at least one Class Member is a citizen of a state different from Defendant, as Plaintiff is a citizen of Kentucky and Defendant is a citizen of Illinois.

4. This Court has personal jurisdiction over Defendant because Roadrunner maintains its principal place of business in this District, regularly conducts business in this District, and is authorized to and does conduct substantial business in this District.

5. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Roadrunner's principal place of business is in this District and a substantial part of the events or omissions giving rise to this action, particularly decisions related to data security and the acts which lead to the Data Disclosure, occurred in this District.

FACTUAL ALLEGATIONS

6. Defendant Roadrunner Transportation Systems, Inc. provides freight transportation and logistics services to small and mid-size shippers throughout North America under the brands Roadrunner®, Active On-Demand®, and Ascent Global Logistics®.

7. Plaintiff and Members of the proposed Class, as current and former employers, relied on Defendant to keep their information stored within the company's employee email system and human resources platform confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

8. In April 2018, Defendant was the subject of a phishing campaign attack via its employee email system ("**Data Breach**"). The attack resulted in the attackers gaining access to Defendant's human resources platform, Workday, and exposed sensitive personally identifying information of employees, including their names, addresses, birthdates, Social Security numbers, financial account information, medical and insurance information, and other types of identifying or sensitive information ("**PII**"). Additionally, the attack resulted in employee direct deposit accounts being changed by the attackers.

9. Defendant became aware of the Data Breach on May 30, 2018 and notified the affected employees on or around July 13, 2018.[1] On or around September 7, 2018, Defendant sent letters to the affected employees offering them twelve (12) months of credit and identity monitoring services.

10. Plaintiff George Nelson is a former employee at Roadrunner whose PII was exposed without his authorization to an unknown attacker as a result of the Data Breach.

11. Within weeks of being notified of the Data Breach, Plaintiff discovered that his PII had been used in connection with the filing of a fraudulent tax return. Plaintiff has spent a significant amount of time addressing the fraudulent tax return that was filed under his name.

12. Concerned that this type of theft could easily happen again, given that his personal information remains in the hands of criminals due to the Data Breach, Plaintiff will have to spend a significant amount of time checking his banking accounts online, monitoring his bank accounts and credit reports and taking other actions necessary to protect himself from future incidents of identity theft or fraud.

13. Without question, the PII of Plaintiff and Class Members, particularly their Social Security numbers and financial account information, was taken for purposes of identity theft, and unfortunately, Defendant's current and former employees are now, and for the rest of their lives will be, at a heightened risk of further identity theft and fraud.

14. Plaintiff brings this class action against Defendant for failing to adequately secure and safeguard the PII of Plaintiff and the Class and for failing to provide timely accurate and adequate notice to Plaintiff and other Class Members as to precisely how and when their

[1] See July 13, 2018 Letter to Office of the New Hampshire Attorney General, attached hereto as Exhibit A.

sensitive personal information had been given to unknown persons.

15. Roadrunner disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the employee email system was safeguarded against phishing attacks, failing to ensure that employees' PII was safeguarded, failing to take available steps to prevent a data breach, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through exposure to an unknown attacker. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

16. Defendant could have prevented this Data Breach. Roadrunner was not without warning as to the existence and constant threat of phishing email scams, yet it failed to implement adequate measures to protect its employees' PII.

17. Roadrunner's negligence in safeguarding its employees' PII is exacerbated by the well-publicized and repeated warnings and alerts of the increasing risk of email scams.

18. On August 27, 2015, the Federal Bureau of Investigation ("FBI") issued a report warning of the increasingly common scam, known as Business Email Compromise, in which companies had fallen victim to phishing emails.[2] Most importantly, this report called attention to the significant spike in scams, also referred to as spoofing, in which cyber criminals send emails that appear to have initiated from the CEO or other top-level executive at the target company.

---

[2] *See, Public Service Announcement, Business Email Compromise*, Alert No. I-082715a-PSA (August 27, 2015), *available at* https://www.ic3.gov/media/2015/150827-1.aspx (last visited November 8, 2017).

19. Business Email Compromise or phishing or spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. For example, spoofed email may purport to be from someone in a position of authority within a company asking for sensitive data such as passwords or employee information that can be used for a variety of criminal purposes. A telltale sign of a spoofing e-mail is an "urgent" request from a company "executive" requesting that confidential information be provided via email.

20. As noted by cybersecurity journalist Brian Krebs, this type of fraud "usually begins with the thieves either phishing an executive and gaining access to that individual's email account or emailing employees from a look-alike domain that is one or two letters off from the company's true domain name." [3]

21. Spoofing fraud has been steadily increasing in recent years. The FBI recently issued an alert stating that from October 2013 through February 2016, law enforcement received reports from over 17,000 victims of "spoofing" scams, which resulted in more than $2.3 billion in losses. Since January 2015, the FBI has seen a 270% increase in identified victims and exposed loss from spoofing scams.[4]

22. Companies can mount several defenses to spoofing scams. These defenses include employee education and technical security barriers. Employee education is the process of adequately making employees aware of common spoofing scams and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only

---

[3] Brian Krebs, *FBI: $2.3 Billion Lost to CEO Email Scams*, KREBS ON SECURITY (April 7, 2016), *available at* http://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/ (last visited November 8, 2017).
[4] *FBI Warns of Dramatic Increase in Business E-Mail Scams* (April 4, 2016), *available at* https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-email-scams (last visited November 8, 2017).

through secure sources to known recipients. Employee education and secure file-transfer protocols provide the easiest method to assist employees in properly identifying fraudulent e-mails and prevent unauthorized access of personal information.

23. From a technical perspective, companies can also greatly reduce the flow of spoofing e-mails by implementing certain security measures governing e-mail transmissions. Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send email on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication that blocks email streams that have not been properly authenticated.

24. Encrypting the files containing Roadrunner employees' PII would have prevented the Data Breach.

25. Despite the widespread prevalence of phishing email scams aimed at obtaining confidential information from employers, Roadrunner provided its employees with unreasonably deficient training on cybersecurity and information transfer protocols prior to the Data Breach.

26. Roadrunner failed to adequately train its employees on even the most basic of cybersecurity protocols, including:

a. How to detect phishing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

b. Effective password management and encryption protocols for internal and external emails;

c. Avoidance of responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to files containing sensitive information;

e. Implementing guidelines for maintaining and communicating sensitive data; and

f. Protecting sensitive employee information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients.

27. Roadrunner's decisions effectively handed criminals the PII of Plaintiff and other Class Members, and put Plaintiff and the Class at serious, immediate and ongoing risk for identity theft and fraud.

28. The Data Breach was caused by Roadrunner's violation of its obligation to abide by best practices and industry standards concerning the security of highly confidential employee data and the storage, use, and transmission of that data. Roadrunner decided not to comply with accepted security standards and allowed its employees' PII to be exposed and compromised by choosing not to implement security measures that could have prevented or mitigated the Data Breach. Roadrunner failed to implement even the most basic of data security practices to require encryption of any data file containing PII sent electronically, even internally within the company.

29. Roadrunner failed to ensure that all personnel in its human resources and payroll departments were made aware of the continuous threat of phishing email scams.

30. Upon discovery, Roadrunner failed to take reasonable steps to clearly and conspicuously inform Plaintiff and the other Class Members of the nature, timing and extent of the Data Breach. By failing to provide adequate timely notice, Roadrunner prevented Plaintiff and Class Members from protecting themselves from the consequences of the Data Breach.

31. Roadrunner was well aware of the risk of identity theft and other damage to its employees if their PII was exposed to unauthorized third parties or otherwise compromised. The

ramifications of Roadrunner's failure to keep its employees' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

32. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[5] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[6]

33. The data compromised in the Roadrunner Data Breach, particularly, Social Security numbers, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. Indeed, the information compromised in the Roadrunner Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, name, employment information, income data, etc.

34. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[7]

---

[5] 17 C.F.R. § 248.201 (2013).

[6] *Id.*

[7] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited November 8, 2017).

35. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police during an arrest.

36. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[8]

37. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

38. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

39. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link

[8] Social Security Administration, Identity Theft and Your Social Security Number, *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited December 30, 2016).

the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[9]

40. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

42. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

43. Despite all the publicly available knowledge of the continued compromises of PII, Roadrunner's approach to maintaining the privacy of its employees' PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

44. Even reimbursing a consumer for certain financial loss due to fraud does not make that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and

---

[9] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited November 8, 2017).

[10] GAO, Report to Congressional Requesters, at 29 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (last visited November 8, 2017).

that "resolving the problems caused by identity theft [could] take more than a year for some victims." [11]

45. To date, Roadrunner has offered its employees only 12 months of credit monitoring service through AllClear. The offered service is inadequate in to protect the Plaintiff and Class Members from the threats they face, particularly in light of the PII stolen.

46. As a result of Roadrunner's failures to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety and emotional distress. They have suffered or are at increased risk of suffering:

a. Unauthorized use and misuse of their PII;

b. The loss of the opportunity to control how their PII is used;

c. The diminution in value of their PII;

d. The compromise, publication and/or theft of their PII;

e. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

f. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

g. The imminent and certain impending injury flowing from potential fraud and

[11] Victims of Identity Theft, 2012 (Dec. 2013) at 10, 11, *available at* https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited October 23, 2018).

identity theft posed by their PII being placed in the hands of criminals;

h. The continued risk to their PII, which remains in the possession of Roadrunner and is subject to further breaches so long as Roadrunner fails to undertake appropriate measures to protect the PII in its possession; and

i. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

47. As a direct and proximate result of Roadrunner's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

48. In all manners of life in this country, time has constantly been recognized as compensable, for many people it is the way they are compensated. Plaintiff and Class Members should be free of having to deal with the consequences of Roadrunner's carelessness.

49. The injuries to the Plaintiff and Class Members were directly and proximately caused by Roadrunner's failure to implement or maintain adequate data security measures for its employees' PII.

CLASS ACTION ALLEGATIONS

50. Plaintiff brings this suit as a class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

51. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All current and former Roadrunner Transportation Systems, Inc. employees whose PII was compromised as a result of the Data Breach.

52. Excluded from the Class are the officers, directors and legal representatives of Roadrunner and the judges and court personnel to whom this case may be assigned and any members of their immediate families.

53. Numerosity. Fed. R. Civ. P. 23(a)(1). The Members of the Class are so numerous that joinder of all members is impractical. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, it is estimated to be at or above 5,000. The exact number is generally ascertainable by appropriate discovery as Roadrunner has knowledge of the employees whose PII was exposed via the Data Breach.

54. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Roadrunner had a duty to protect the PII of Class Members;

b. Whether Roadrunner had a duty to not expose the PII of Class Members to unauthorized third parties;

c. Whether Roadrunner had a duty to not use the PII of Class Members for non-

business purposes;

d. Whether Roadrunner failed to adequately safeguard the PII of Class Members;

e. Whether Roadrunner adequately, promptly, and accurately informed Class Members that their PII had been compromised;

f. Whether Roadrunner failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information exposed through the Data Breach;

g. Whether Roadrunner engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Class Members;

h. Whether Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Roadrunner's wrongful conduct;

j. Whether Plaintiff and the Members of the Class are entitled to restitution as a result of Roadrunner's wrongful conduct; and,

k. Whether Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

55. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was exposed by Roadrunner. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class Members arise from the same operative facts and are based on the same legal theories.

56. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

57. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Roadrunner. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical.

58. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would

be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Member of the Class to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

59. The litigation of the claims brought herein is manageable. Defendant's uniform misconduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

60. Adequate notice can be given to Class Members directly using information maintained in Roadrunner's records.

61. Unless a Class-wide injunction is issued, Roadrunner may continue authorized exposure of the PII of Class Members, Roadrunner may continue in its failure to properly secure the PII of Class Members, Roadrunner may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Roadrunner may continue to act unlawfully as set forth in this Complaint.

62. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

63. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, transmitting, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, transmitting, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately, and accurately informed Class Members that their PII had been exposed without authorization;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed and compromised in the Data Breach;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard and exposing without authorization the PII of Class Members; and,

g. Whether Class Members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

64. Plaintiff realleges paragraphs 1through 63 above as if fully set forth here.

65. As a condition of their employment, employees were obligated to provide Roadrunner with certain PII, including their date of birth, mailing addresses and Social Security numbers.

66. Plaintiff and the Class Members entrusted their PII to Roadrunner on the premise and with the reasonable expectation and understanding that Roadrunner would safeguard their information, use their PII for business purposes only, and/or not expose their PII to unauthorized third parties.

67. Roadrunner's obligation under federal law to collect PII from its employees was accompanied by a duty to use reasonable care in the protection, use, transmission, and safeguarding of this PII.

68. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully exposed.

69. Roadrunner knew or reasonably should have known that the failure to exercise due care in the collecting, storing, transmitting, and using of its employees' PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the acts of a third party.

70. Roadrunner knew or reasonably should have known of the government and industry warnings regarding the prevalence of phishing email scams seeking information of employees and that the failure to heed these warnings would create an unreasonable risk of harm to Plaintiff and Class Members.

71. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or exposed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing Defendant's security protocols to ensure that Plaintiff and Class Members' information in its possession was adequately secured and protected and that employees tasked with maintaining such information and the employee email system were adequately training on cyber security

measures regarding the security of employees' personal information.

72. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Roadrunner knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the current cyber scams being perpetrated on companies, and that it had an inadequate employee email system and inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiff and the Class.

73. Roadrunner's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Roadrunner's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Roadrunner's misconduct also included its decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class Members.

74. Plaintiff and Class Members had no ability to protect their PII that was in Roadrunner's possession.

75. Roadrunner was in the sole position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

76. Roadrunner had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within its possession was exposed without authorization, might have been compromised, how it was exposed and/or compromised and precisely the types of information that were disclosed and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate and repair any identity theft and the fraudulent use of their PII by third parties.

77. Roadrunner had a duty to have proper procedures in place to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

78. Roadrunner has acknowledged that the PII of Plaintiff and Class Members was wrongfully exposed to unauthorized third persons as a result of the Data Breach.

79. Roadrunner, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Roadrunner's possession or control.

80. Roadrunner improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations and practices at the time of the Data Breach.

81. Roadrunner failed to heed industry warnings and alerts issued by the government and other resources to provide adequate safeguards to protect employees' PII in the face of increased risk of phishing email scams.

82. Roadrunner, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect phishing email scams and to prevent the unauthorized exposure of its employees' PII.

83. Roadrunner, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence, and scope of the Data Breach.

84. But for Roadrunner's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been exposed and compromised.

85. There is a close causal connection between Roadrunner's decision not to implement security measures to protect the PII of current and former employees and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class.

86. As a result of Roadrunner's negligence, Plaintiff and Class Members have suffered and will continue to suffer damages and injury including, but not limited to: identity theft, out-of-pocket expenses associated with procuring robust credit monitoring and identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

SECOND CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

87. Plaintiff realleges paragraphs 1through 63 above as if fully set forth here.

88. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against exposure to unauthorized third parties.

89. Because of the nature of the relationship between Defendant and its employees, including that Defendant is required by law to obtain certain PII of its employees and employees are required to provide such data to Defendant, Defendant owed a duty to its employees, including Plaintiff and Class Members, to keep their PII confidential and prevent unauthorized exposure of such PII.

90. The unauthorized disclosure to unauthorized third parties of the PII of Plaintiff and Class Members, especially where the information includes Social Security numbers and financial information, would be highly offensive to a reasonable person.

91. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Roadrunner as part of their employment, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized exposure. Plaintiff and Class Members were reasonable to believe that such information would be kept private and would not be exposed without their authorization.

92. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

93. As a proximate result of the above acts and omissions of Roadrunner, the PII of Plaintiff and Class Members was exposed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

94. Unless and until enjoined, and restrained by order of this Court, Roadrunner's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Roadrunner can be viewed, distributed and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

95. Plaintiff realleges paragraphs 1through 63 above as if fully set forth here.

96. Plaintiff and Class Members were required to provide their PII, including names,

addresses, Social Security numbers, and other personal information, to Roadrunner as a condition of their employment.

97. Implicit in the employment agreement between Defendant and its employees was the obligation that Roadrunner would use the PII of its employees for business purposes only and not make unauthorized disclosures of the information.

98. Roadrunner had an implied duty to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses.

99. Additionally, by accepting the PII of its employees, Roadrunner implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

100. Plaintiff and Class Members fully performed their obligations under the implied contract with Roadrunner. Defendant did not.

101. Roadrunner breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' PII, which was exposed to unauthorized third parties by Roadrunner's inadequate safeguarding of the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations and practices regarding data security.

102. Roadrunner's acts and omissions have materially affected the intended purpose of the implied contacts requiring Plaintiff and Class Members to provide their PII as a condition of employment in exchange for compensation and benefits.

103. As a direct and proximate result of Roadrunner's breach of its implied contacts with Plaintiff and Class Members, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the control over how their PII is used and who

has access to same; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their PII, which remains in Roadrunner's possession and is subject to further unauthorized disclosures so long as Roadrunner fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and, (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

104. Plaintiff realleges paragraphs 1through 63 above as if fully set forth here.

105. In light of the special relationship between Roadrunner and its employees, whereby Roadrunner required Plaintiff and Class Members to provide highly sensitive, confidential, personal and financial information as a condition of their employment, Roadrunner was a fiduciary, as an employer created by its undertaking, to act primarily for the benefit of its employees, including Plaintiff and Class Members, for the safeguarding of employees' PII and financial information.

106. Roadrunner had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their employer/employee relationship, in particular to

keep secure financial records and the PII of its employees.

107. Roadrunner breached its duty of care to Plaintiff and Class Members to ensure that their PII was not exposed without authorization or used for improper purposes by failing to provide adequate safeguards of their PII in deviation of standard industry rules, regulations and practices regarding data security, which resulted in exposure of employees' PII to unauthorized third parties.

108. As a direct and proximate result of Roadrunner's actions alleged above, Plaintiff and Class Members have suffered actual damages.

FIFTH CAUSE OF ACTION
Violation of Illinois Personal Information Protection Act,
815 Ill. Comp. Stat. 530/1 *et seq.*
(On Behalf of Plaintiff and the Class)

109. Plaintiff realleges paragraphs 1through 63 above as if fully set forth here.

110. By being headquartered in Illinois, employing Illinois residents, and collecting and storing the PII of those Illinois residents, Roadrunner is obligated to comply with the Illinois Personal Information Protection Act, 815 Ill. Comp. Stat. 530/1 *et seq*. ("**IPIPA**").

111. Roadrunner is a "data collector" under the provisions of IPIPA.

112. IPIPA requires a data collector that "maintains or stores… records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, … use, … or disclosure." IPIPA, 815 Ill. Comp. Stat. 530/45(a).

113. As detailed above, Roadrunner violated the IPIPA by exposing its employees' PII to unauthorized third parties.

114. As detailed above, Roadrunner violated the IPIPA by making the voluntary

decision not to implement and maintain reasonable security measures to prevent the unauthorized exposure of its employees' PII.

115. Roadrunner improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations and practices regarding data security and data transmission at the time of the Data Breach.

116. Roadrunner failed to heed industry warnings and alerts issued by the government and other resources to provide adequate safeguards to protect employees' PII in the face of increased risk of phishing email scams.

117. Roadrunner, through its actions and/or omissions, violated the IPIPA by failing to have appropriate procedures in place to detect phishing email scams and to prevent unauthorized exposure of its employees' PII.

118. As a direct and proximate result of Roadrunner's actions alleged above, Plaintiff and Class Members have suffered actual damages.

SIXTH CAUSE OF ACTION
Violation of Illinois Consumer Fraud and Deceptive Business Practices Act,
815 Ill. Comp. Stat. 505/1 *et seq.*
(On Behalf of Plaintiff and the Class)

119. Plaintiff realleges paragraphs 1through 63 above as if fully set forth here.

120. The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 530/20 ("**ICFA**") provides that a violation of the IPIPA "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

121. As detailed above, through its acts and omissions, Roadrunner violated the IPIPA by failing to implement and maintain reasonable security measures to prevent the unauthorized exposure of its employees' PII. Accordingly, Roadrunner's violation of the IPIPA constitutes a

violation of the ICFA.

122. Further, Plaintiff and the other Members of the Class were deceived by Roadrunner's failure to properly implement adequate, commercially reasonable security measures to protect its employees' PII.

123. Roadrunner intended for its employees, including Plaintiff and other Members of the Class, to rely on Roadrunner to protect the PII furnished to it in connection with their employment and to store, use, and transmit the PII for business purposes only and only as authorized.

124. Instead, Roadrunner allowed the unauthorized exposure of its employees' PII to unknown third parties.

125. Roadrunner failed to follow industry best practices concerning security in the storage, use, and transmission of PII or was negligent in preventing the Data Breach from occurring.

126. By inadequately safeguarding the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations and practices regarding data security and data transmission, it was foreseeable to Roadrunner that unknown third parties could gain unfettered and unlimited access to, examination of, and use of highly confidential PII of Plaintiff and Class Members.

127. It was foreseeable to Roadrunner that its willful indifference or negligent course of conduct in handling its employees' PII would put that information at risk of compromise or unauthorized exposure.

128. Defendant's fraudulent and deceptive acts and omissions were intended to induce Plaintiff and the other Class Members' reliance on Defendant's deception that their PII

information was secure and protected and would only be disclosed as authorized when providing Roadrunner this personal data as a condition of employment.

129. Roadrunner violated the ICFA by failing to properly implement adequate, commercially reasonable security measures to protect its employees' PII from unauthorized disclosure, by failing to warn its employees that their information was at risk of being compromised or disclosed without authorization, and by failing to discover and immediately notify its employees of the nature and extent of the Data Breach.

130. Plaintiff and Members of the Class have suffered injury in fact and actual damages as a result of Roadrunner's violations of the ICFA.

PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of himself and all others similarly situated, prays for relief as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and his Counsel to represent the Class;

B. A mandatory injunction directing Roadrunner to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;

C. A mandatory injunction requiring that Roadrunner provide notice to each Member of the Class relating to the full nature and extent of the Data Breach and the exposure of PII to unauthorized persons;

D. For an award of damages, in an amount to be determined;

E. For an award of attorneys' fees and costs;

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: November 7, 2018

Respectfully submitted,

MORGAN & MORGAN COMPLEX LITIGATION GROUP

/s/ John A. Yanchunis
John A. Yanchunis
jyanchunis@forthepeople.com
Jonathan B. Cohen*
jcohen@forthepeople.com
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

CLIFFORD LAW OFFICES, P.C.

/s/ Shannon M. McNulty
Shannon M. McNulty
smm@cliffordlaw.com
Robert A. Clifford
rclifford@cliffordlaw.com
120 N. LaSalle Street, Suite 3100
Chicago, IL 60602
Telephone: (312) 899-9090
Facsimile: (312) 251-1160

Attorneys for Plaintiff and the Proposed Class

* *pending pro hac vice* admission

Exhibit A

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.

ILND 44 (Rev. 09/07/18)

CIVIL COVER SHEET

The ILND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(See instructions on next page of this form.)*

I. (a) PLAINTIFFS

George Nelson, on behalf of himself and all other similarly situated,

(b) County of Residence of First Listed Plaintiff: Green County
(Except in U.S. plaintiff cases)

(c) Attorneys *(firm name, address, and telephone number)*

Clifford Law Offices, P.C. 120 N. LaSalle St., Chicago 60602 (312) 899-9090
Morgan & Morgan Complex Litigation Group, 201 N. Franklin St., Tampa, FL 33602 (813) 223-5505

DEFENDANTS

Roadrunner Transportation Systems, Inc.

County of Residence of First Listed Defendant: Cook
(In U.S. plaintiff cases only)
Note: In land condemnation cases, use the location of the tract of land involved.

Attorneys *(if known)*

II. BASIS OF JURISDICTION *(Check one box, only.)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government not a party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate citizenship of parties in Item III.)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(For Diversity Cases Only.)*

(Check one box, only for plaintiff and one box for defendant.)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business in This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business in Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Check one box, only.)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 530 General
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

PRISONER PETITIONS
- ☐ 510 Motions to Vacate Sentence
- 530 General
- ☐ 535 Death Penalty

Habeas Corpus:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee – Conditions of Confinement

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent – Abbreviated New Drug Application
- ☐ 840 Trademark

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729 (a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act (TCPA)
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 463 Habeas Corpus - Alien Detainee (Prisoner Petition)
- ☐ 465 Other Immigration Actions

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- 690 Other

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAXES
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

V. ORIGIN *(Check one box, only.)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation ☐ 8 Multidistrict Litigation Direct File

VI. CAUSE OF ACTION

(Enter U.S. Civil Statute under which you are filing and write a brief statement of cause.)

28 U.S.C. 1332(d)

VII. PREVIOUS BANKRUPTCY MATTERS

(For nature of suit 422 and 423, enter the case number and judge for any associated bankruptcy matter previously adjudicated by a judge of this Court. Use a separate attachment if necessary.)

VIII. REQUESTED IN COMPLAINT:

☒ Check if this is a **class action** Under rule 23, F.R.CV.P. **Demand $**

Check Yes only if demanded in complaint.
Jury Demand: ☒ Yes ☐ No

IX. RELATED CASE(S) IF ANY *(See instructions)*

Judge: Case Number:

X. Is this a previously dismissed or remanded case? ☐ Yes ☒ No If yes, Case # Name of Judge

Date: 11/07/2018

Signature of attorney of record: /s/Shannon M. McNulty