UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

CLARA HUGHES-HILLMAN, individually and on behalf of all others similarly situated, Plaintiff, v. SONIC CORPORATION, Defendant.	Civil Action No. DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff CLARA HUGHES-HILLMAN ("Plaintiff"), individually and on behalf of the Classes of similarly situated persons defined below, allege the following against Sonic Corporation ("Sonic" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE CASE

1. This is a consumer class action against Sonic for its failure to secure and safeguard the credit and debit card numbers and other payment card data, and other personally identifiable information (collectively, "PII") that Sonic collected from Plaintiff and other Class members (the "Customer Data") when they made purchases at Sonic.

2. On September 26, 2017, Sonic announced that its payment system had been breached and that PII consisting of up to five million credit card and debit card numbers and other personally identifying information had been stolen (the "Data Breach") .

3. The stolen PII is being sold on the black market. The stolen Customer Data is sufficient for wrongdoers to make fraudulent charges to the accounts of Plaintiff and the Class members.

4. This Customer Data was compromised due to Sonic's acts and omissions and its failure to properly protect the Customer Data.

5. Data breaches at other restaurants, including Sonic's competitors, have occurred and were widely publicized, putting Sonic on notice that it might be the target of a cybersecurity attack like the Data Breach.

6. Sonic could have prevented the Data Breach. Sonic disregarded the rights of Plaintiff and Class members by: (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected; (ii) failing to take available steps to prevent and stop the breach from happening; (iii) failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard Customer Data; (iv) failing to take available steps to prevent and stop the breach from ever happening; and (v) failing to monitor and detect the breach on a timely basis.

7. Had Sonic implemented and maintained adequate safeguards to protect Customer Data, deter the hackers, and detect the beach within a reasonable amount of time, it is more likely than not that it would have been able to prevent the Data Breach.

8. As a result of the Data Breach, the Customer Data of Plaintiff and the Class members has been exposed to criminals and is ripe for misuse. The injuries suffered by Plaintiff and Class members as a direct result of the Data Breach include:

a. the unauthorized use of their Customer Data (e.g., unauthorized charges to their debit and credit card accounts);

b. the theft of their personal and financial information;

c. the costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. the damages arising from the inability to use debit or credit card accounts because those account were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Data Breach (e.g., the loss of cash back rewards);

e. the loss of use of and access to account funds and the costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects to their credit (e.g., decreased credit scores and adverse credit notations);

f. the costs associated with time spent attempting to mitigate the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress and nuisance of dealing with issues caused by the Data Breach;

g. the imminent and impending injury flowing from fraud and identify theft as the result of their credit card and personal information being placed in the hands of criminals—indeed, Plaintiff's and Class members' Customer Data was already being sold on the Internet black market the day that Sonic announced the Data Breach;

h. the damages to and diminution in value of their PII, which was entrusted to Sonic for the sole purpose of purchasing products and services from Sonic and with the mutual

understanding that Sonic would safeguard Plaintiff's and Class members' Customer Data against theft and not allow others to access and misuse their information;

i. the money paid for products and services purchased at Sonic stores during the period of the Data Breach, in that Plaintiff and Class members would not have shopped at Sonic had Sonic disclosed that it lacked adequate systems and procedures to reasonably safeguard Customer Data; and

j. the continued risk that their Customer Data, which remains in the possession of Sonic, will be breached again. The Customer Data is subject to further breaches so long as Sonic fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' Customer Data in its possession.

9. The injuries to the Plaintiff and members of the Classes were directly and proximately caused by Sonic's failure to implement or maintain adequate data security measures for the Customer Data. Sonic failed to take steps to employ adequate security measures despite recent, well-publicized data breaches at large national retail and restaurant chains, including Arby's, P.F. Chang's, Wendy's, Dairy Queen, and Noodles & Company. Furthermore, Sonic exacerbated the situation by failing to detect the Data Breach earlier. Had Sonic detected the breach earlier, less data would have been stolen and customers would have been able to take earlier action to mitigate their damages.

10. Plaintiff retains a significant interest in ensuring that her Customer Data, which, while stolen, remains in the possession of Sonic, is protected from further breaches, and seeks to remedy the harms she has suffered on behalf of herself and similarly situated consumers whose Customer Data was stolen as a result of the Data Breach.

11. Plaintiff, on behalf of herself and similarly situated consumers, seek to recover damages, equitable relief (including injunctive relief to prevent a reoccurrence of the Data Breach and the injuries flowing therefrom), restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. Sonic and at least one Plaintiff are citizens of different states. There are more than 100 putative class members.

13. This Court has personal jurisdiction over Defendant because Sonic regularly conducts business in Illinois, operating 47 restaurants throughout the state, and has sufficient minimum contacts in Illinois.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because substantial parts of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District

PARTIES

15. Plaintiff Clara Hughes-Hillman is a resident of Chicago, Illinois, and was an Illinois resident during the period of the Data Breach. On August 8, 2016, August 24, 2016 and September 7, 2016, Plaintiff purchased food at a Sonic Drive-In located at 10440 Grand Ave. Franklin Park, IL 60131, with a Visa debit card that was swiped through a Sonic point-of-sale payment device.

16. Plaintiff would not have used her credit or debit cards to make purchases at Sonic—indeed, she would not have shopped at Sonic at all during the period of the Data Breach—had Sonic told her that it lacked adequate computer systems and data security practices to safeguard customers' PII from theft.

17. Plaintiff suffered actual injury from having her Customer Data stolen in and as a result of the Data Breach.

18. Plaintiff suffered actual injury and damages in paying money to and purchasing products from Sonic during the Data Breach, expenditures which she would not have made had Sonic disclosed that it lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

19. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Customer Data—a form of intangible property that Plaintiff entrusted to Sonic for the purpose of purchasing its products and that was compromised in and as a result of the Data Breach.

20. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals. Indeed, the criminals have already misused the stolen Customer Data by selling Plaintiff's and Class members' PII on the dark web. Plaintiff has a continuing interest in ensuring that her PII, which remains in the possession of Sonic, is protected and safeguarded from future breaches.

21. Plaintiff is likely to purchase food or services from Sonic with a credit or debit card in the future if Sonic's data security is improved to protect against future data breaches.

22. Defendant Sonic Corporation is a Delaware corporation with its principal place of business located at 300 Johnny Bench Drive, Oklahoma City, OK 73104. Sonic is publicly traded on the NASDAQ National Market Stock Exchange under the ticker SONC.

23. Sonic's restaurant system consists of over 3,500 corporate-owned and franchisee locations across the U.S. and worldwide. Approximately 345 of these are corporate-owned restaurants and the remainder are franchised. Sonic restaurants accept payment for their goods and services through a POS system, through which customers swipe credit and debit cards to pay.

STATEMENT OF FACTS

24. Sonic is the largest chain of drive-in restaurants in the United States. It operates over 3,500 restaurants in 44 states. Sonic accepts credit and debit card payments from its customers.

25. On September 26, 2017, Sonic announced that its payment system had been breached and up to five million credit card and debit card accounts had been stolen. *See* https://www.sonicdrivein.com/-/notice-of-data-breach.

26. The stolen PII was already being sold on the black market on the day Sonic announced the Data Breach. *See* https://krebsonsecurity.com/2017/09/breach-at-sonic-drive-in-may-have-impacted-millions-of-credit-debit-cards/.

27. Criminals can use the stolen PII to make fraudulent charges to Sonic customers' accounts. *See* http://www.securityweek.com/breach-fast-food-chain-sonic-couldimpact-millions-report.

28. There have been high profile data breaches of other restaurant chains, putting Sonic on notice of the need to take steps to prevent data breaches. *See* https://www.qsrmagazine.com/restaurant-software/7-ways-protect-against-data-breach.

29. The payment system used by Sonic was more than thirty years old. While the company has been working to update its system, many restaurant locations have not yet been updated. *See* http://www.nrn.com/technology/sonic-team-helps-operators-reap-benefits-new-pos-system.

30. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse posed by her PII being placed in the hands of criminals who have already, or will imminently, misuse such information.

31. Plaintiff has a continuing interest in ensuring that her PII, which remains in the possession of Sonic, is protected and safeguarded from future breaches.

32. At all relevant times, Sonic was aware, or reasonably should have been aware, that the PII collected, maintained and stored in the POS systems is highly sensitive, susceptible to attack, and could be used by third parties for wrongful purposes, such as identity theft and fraud.

33. It is well-known and the subject of many media reports that PII is highly coveted and a frequent target of hackers.

34. Despite the frequent public announcements of data breaches of other restaurants, Sonic continued to use an outdated, insufficient, and inadequate system to protect the Customer Data of Plaintiff and Class members.

35. PII is a valuable commodity. A "cyber black market" exists in which criminals openly post stolen payment card numbers and other PII on a number of underground Internet websites. PII is "as good as gold" to identity thieves because they can use victims' personal data to incur charges on existing accounts, or clone ATM, debit, and credit cards. Data from the Sonic breach has already appeared on such sites. *See* http://www.securityweek.com/breach-fast-food-chain-sonic-could-impactmillions-report.

36. Legitimate organizations and the criminal underground alike recognize the value of PII contained in a merchant's data systems. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[1] 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."[2]

[1] 17 C.F.R § 248.201 (2013).

[2] *Id.*

37. PII is a valuable commodity to identity thieves. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[3]

38. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[4]

39. At all relevant times, Sonic knew, or reasonably should have known, of the importance of safeguarding the Customer Data and of the foreseeable consequences of the breach of its data security system by hackers, including, specifically, the significant costs that would be imposed on its customers as a result of such a breach.

40. Sonic was, or should have been, fully aware of the significant number of people whose PII it collected and, thus, the significant number of individuals who would be harmed by a breach of its payment system.

41. Unfortunately, and as alleged below, despite the numerous and well-publicized examples of cybersecurity breaches in the computer systems of its competitors, and the harm that is done to customers when PII falls into the hands of hackers, Sonic's approach to maintaining the privacy and security of the Customer Data of Plaintiff and Class members was reckless and negligent.

42. The ramifications of Sonic's failure to secure the Customer Data secure are severe. Reimbursing a consumer for a financial loss due to identity fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own

---

[3] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 10, 2017).

[4] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud- hits-inflectionpoint (last visited April 10, 2017).

money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[5]

43. There may be a time lag between when the harm occurs and 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.[6]

44. 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.

45. The PII of Plaintiff and Class members is private and sensitive in nature and was inadequately protected by Sonic.

46. The Data Breach was a direct and proximate result of Sonic's failure to properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law.

---

[5] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 10, 2017).

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

47. Sonic failed to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

48. Sonic had the resources to prevent a breach, but neglected to timely and adequately invest in data security, despite the growing number of well-publicized data breaches.

49. Had Sonic remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Sonic would have prevented the Data Breach and, ultimately, the theft of the Customer Data.

50. As a direct and proximate result of Sonic'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 identity theft, requiring them to take the time 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. The loss of time has been recognized as a compensable injury.

51. Sonic's wrongful actions and inaction directly and proximately caused the theft and dissemination of the Customer Data, causing Plaintiff and members of the Class to suffer, and continue to suffer, economic damages and other actual harm, including:

a. the unauthorized use of their Customer Data (e.g., unauthorized charges to their debit and credit card accounts);

b. the theft of their personal and financial information;

c. the costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. the damages arising from the inability to use debit or credit card accounts because those account were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Data Breach (e.g., the loss of cash back rewards);

e. the loss of use of and access to account funds and the costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects to their credit (e.g., decreased credit scores and adverse credit notations);

f. the costs associated with time spent attempting to mitigate the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress and nuisance of dealing with issues caused by the Data Breach;

g. the imminent and impending injury flowing from fraud and identify theft as the result of their credit card and personal information being placed in the hands of criminals—indeed, Plaintiff's and Class members' Customer Data was already being sold on the Internet black market the day that Sonic announced the Data Breach;

h. the damages to and diminution in value of their PII, which was entrusted to Sonic for the sole purpose of purchasing products and services from Sonic and with the mutual understanding that Sonic would safeguard Plaintiff's and Class members' Customer Data against theft and not allow others to access and misuse their information;

i. the money paid for products and services purchased at Sonic stores during the period of the Data Breach, in that Plaintiff and Class members would not have shopped at Sonic had Sonic disclosed that it lacked adequate systems and procedures to reasonably safeguard Customer Data; and

j. the continued risk that their Customer Data, which remains in the possession of Sonic, will be breached again. The Customer Data is subject to further breaches so long as Sonic fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' Customer Data in its possession.

52. Sonic continues to hold the PII of its customers, including Plaintiff and Class members. Plaintiff and members of the Class have an undeniable interest in insuring that their PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft—particularly because Sonic has demonstrated an inability to prevent a breach or stop it after being detected.

CLASS ALLEGATIONS

53. Plaintiff seeks relief on behalf of herself as representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and (c)(4), Plaintiff seeks certification of a nationwide class defined as follows:

> All persons residing in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Sonic in September 2017 (the "Nationwide Class").

54. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims under the laws of Illinois, and on behalf of a separate statewide class, defined as follows:

> All persons residing in Illinois whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Sonic in September 2017 (the "Statewide Class").

55. Excluded from each of the above Classes are any of Sonic's officers, directors, and board members; all persons who make a timely election to be excluded from the Class; and the judges to whom this case is assigned and their immediate family.

56. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

57. The members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, the proposed Class include several million individuals across the country whose PII was compromised in the Data Breach. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

58. This action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether Sonic had a duty to protect the PII in its possession;

b. Whether Sonic knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Sonic's security measures to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Sonic was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Sonic's failure to implement reasonable and adequate data security measures allowed the breach to occur;

f. Whether Sonic's conduct constituted deceptive trade practices under state law;

g. Whether Sonic's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiff and Class members;

h. Whether Plaintiff and Class members were injured and suffered damages or other losses because of Sonic's failure to reasonably protect its POS systems and data network; and,

i. Whether Plaintiff and Class members are entitled to relief.

59. Plaintiff's claims are typical of those of other Class members. Plaintiff had her PII compromised in the Data Breach. Plaintiff's damages and injuries are akin to other Class members and Plaintiff seeks relief consistent with the relief of the Class.

60. Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Sonic to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

61. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Sonic, and thus, individual litigation to redress Sonic's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system.

Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

62. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

63. 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 Sonic owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether Sonic's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

c. Whether Sonic failed to adequately comply with industry standards and, if so, whether that failure amounted to negligence;

d. Whether Sonic failed to take commercially reasonable steps to safeguard the PII of Plaintiff and the Class members; and,

e. Whether adherence to data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

64. All members of the proposed Classes are readily ascertainable. Sonic has access to information regarding the Data Breach, the time period of the Data Breach, and which individuals

were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

COUNT I

NEGLIGENCE (ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SEPARATE STATEWIDE CLASS)

65. Plaintiff restates and re-alleges Paragraphs 1 through 64 as if fully set forth herein.

66. Upon accepting and storing the PII of Plaintiff and Class Members in its computer systems and on its networks, Sonic undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Sonic knew that the PII was private and confidential and should be protected as such.

67. Sonic owed a duty of care not to subject Plaintiff and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

68. Sonic owed numerous duties to Plaintiff and to members of the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

69. Sonic also breached its duty to Plaintiff and the Class Members to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite

obvious risks. Further, Sonic failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather the PII of Plaintiff and Class Members, misuse the Customer Data, and intentionally disclose it to others without consent.

70. Sonic knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Sonic knew about numerous, well-publicized data breaches, including the breaches at Wendy's, Chipotle, Arby's, and others.

71. Sonic knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

72. Sonic breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members.

73. Because Sonic knew that a breach of its systems would damage millions of individuals, including Plaintiff and Class members, Sonic had a duty to adequately protect their data systems and the PII contained thereon.

74. Sonic's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PII. Sonic's misconduct included failing to: (i) secure its systems, despite knowing their vulnerabilities, (ii) comply with industry standard security practices, (iii) implement adequate system and event monitoring, and (iv) implement the systems, policies, and procedures necessary to prevent this type of data breach.

75. Sonic also had independent duties under state and/or federal laws that required it to safeguard Plaintiff's and Class members' PII.

76. Sonic breached its duties to Plaintiff and Class members in numerous ways, including: (i) by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiff and Class members; (ii) by creating a foreseeable risk of harm through the misconduct previously described; (iii) by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' PII both before and after learning of the Data Breach; and (iv) by failing to comply with the minimum industry data security standards during the period of the Data Breach.

77. Through Sonic's acts and omissions described in this Complaint, including Sonic's failure to provide adequate security and its failure to protect the PII of Plaintiff and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Sonic unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiff and Class members during the time it was within its possession or control.

78. Upon information and belief, Sonic improperly and inadequately safeguarded PII of Plaintiff and Class Members, deviating from standard industry rules, regulations, and practices at the time of the unauthorized access. Sonic's failure to take proper security measures to protect the PII of Plaintiff and Class members created conditions conducive to a foreseeable criminal act—unauthorized access to the PII of Plaintiff and Class members.

79. Sonic's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiff and Class members; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive PII had been compromised.

80. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

81. As a direct and proximate cause of Sonic's conduct, Plaintiff and the Class members suffered injuries including, but not limited to: (i) damages arising from the unauthorized charges on debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Class Members; (ii) damages arising from Plaintiff's and the Class' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach (including but not limited to late fees and foregone cash back rewards); (iii) damages from time spent and effort expended to mitigate the actual and potential impact of the Data Breach 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; and (iv) damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II

NEGLIGENCE PER SE (ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SEPARATE STATEWIDE CLASS)

82. Plaintiff restates and reallege Paragraphs 1 through 81 as if fully set forth herein.

83. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as

Sonic, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Sonic's duty in this regard.

84. Sonic violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

85. Sonic's violation of Section 5 of the FTC Act constitutes negligence per se.

86. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

87. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

88. As a direct and proximate result of Sonic's negligence per se, Plaintiff and the Class have suffered, and continue to suffer, injuries including, but not limited to: (i) damages arising from the unauthorized charges on debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Class Members; (ii) damages arising from Plaintiff's and the Class' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach (including but not limited to late fees and foregone cash back rewards); (iii) damages from time spent and effort expended to mitigate the actual and potential impact of the Data Breach 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; and (iv) damages from identity theft, which may take months if not years to

discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT III

DECLARATORY JUDGMENT (ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SEPARATE STATEWIDE CLASS)

89. Plaintiff restates and realleges Paragraphs 1 through 88 as if fully set forth herein.

90. As previously alleged, Plaintiff and Class members entered into an implied contract that required Sonic to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Sonic owes duties of care to Plaintiff and Class members that require it to adequately secure PII.

91. Sonic still possesses the PII of Plaintiff and Class members.

92. Sonic has made no announcement or notification that it has remedied the vulnerabilities in its computer systems and networks.

93. Accordingly, Sonic has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Sonic's lax approach towards data security has become public, the PII in its possession is more vulnerable than ever.

94. Actual harm has arisen in the wake of the Data Breach regarding Sonic's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

95. Plaintiff, therefore, seeks a declaration that (a) Sonic's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Sonic must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on

Sonic's systems on a periodic basis, and ordering Sonic to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access controls so that if one portion of Sonic's computer system or network is compromised, hackers cannot gain access to other portions of Sonic's computer system or network ;

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for the provisions of its services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Sonic customers must take to protect themselves.

COUNT IV

VIOLATION OF OKLAHOMA CONSUMER PROTECTION ACT, 15 O.S. § 751 ET SEQ. (the "OCPA") (ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SEPARATE STATEWIDE CLASS)

96. Plaintiff restates and realleges Paragraphs 1 through 95 as if fully set forth herein.

97. Sonic is headquartered and engaged in business in Oklahoma. Sonic's response to, and corporate decisions surrounding such response to, the Data Breach were made from and in Oklahoma.

98. Oklahoma, which seeks to protect the rights and interests of Oklahomans and others against a company doing business in Oklahoma, has an interest in the claims of Plaintiff and the Class members and is intimately concerned with the claims and outcome of this litigation. Accordingly, Plaintiff and the Class assert claims under the OCPA.

99. Plaintiff and Class members entrusted Sonic with their PII.

100. As alleged herein, Sonic engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the OCPA:

a. failure to maintain the security of credit and/or debit card account information;

b. failure to maintain adequate computer systems and data security practices to safeguard credit and debit card information and other PII;

c. failure to disclose that its computer systems and data security practices were inadequate to safeguard credit and debit card information and other PII from theft;

d. continued acceptance of PII and storage of other personal information after Sonic knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach;

e. allowing unauthorized persons to have access to and make unauthorized charges to its customers' credit and/or debit card accounts.

101. Sonic knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

102. As a direct and proximate result of Sonic's violation of the OCPA, Plaintiff and Class members suffered injuries including, but not limited to: (i) damages arising from the unauthorized charges on debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Class Members; (ii) damages arising from Plaintiff's and the Class' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach (including but not limited to late fees and foregone cash back rewards); (iii) damages from time spent and effort expended to mitigate the actual and potential impact of the Data Breach 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; and (iv) damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

103. Also as a direct result of Sonic's knowing violation of the OCPA, Plaintiff and Class members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Sonic engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Sonic's systems on a periodic basis, and ordering Sonic to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Sonic engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Sonic audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Sonic segment PII by, among other things, creating firewalls and access controls so that if one area of Sonic is compromised, hackers cannot gain access to other portions of Sonic systems;

e. Ordering that Sonic purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Sonic conduct regular database scanning and securing checks;

g. Ordering that Sonic routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Sonic to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Sonic customers must take to protect themselves.

104. Plaintiff brings this action on behalf of herself and Class Members for the relief requested above and to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and Class members and the public from Sonic's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Sonic's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

105. Plaintiff and Class members are entitled to a judgment against Sonic for actual and consequential damages, exemplary damages and attorneys' fees pursuant to the OCPA, costs, and such other further relief as the Court deems just and proper.

COUNT IV

VIOLATION OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS § 505/1 ET SEQ. (the "ICFA") (ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE SEPARATE STATEWIDE CLASS)

106. Plaintiff restates and realleges Paragraphs 1 through 105 as if fully set forth herein.

107. Sonic is engaged in trade or commerce in Illinois. Plaintiff conducted business with Sonic in Illinois.

108. Illinois, which seeks to protect the rights and interests of Illinoisans and others against a company doing business in Illinois, has an interest in the claims of Plaintiff and the Class members and is intimately concerned with the claims and outcome of this litigation. The intent of the ICFA is "to protect consumers, borrowers, and business persons against fraud, unfair methods, of competition, and other unfair and deceptive business practices."[7] Accordingly, Plaintiff and the Class assert claims under the ICFA.

109. Plaintiff and Class members entrusted their PII to Sonic.

110. As alleged herein, Sonic engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the ICFA:

a. failure to maintain the security of credit and/or debit card account information;

b. failure to maintain adequate computer systems and data security practices to safeguard credit and debit card information and other PII;

[7] *Siegel v. Shell Oil Co.*, 612 F.3d 932, 934 (7th Cir.2010)

c. failure to disclose that its computer systems and data security practices were inadequate to safeguard credit and debit card information and other PII from theft;

d. continued acceptance of PII and storage of other personal information after Sonic knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach;

e. allowing unauthorized persons to have access to and make unauthorized charges to its customers' credit and/or debit card accounts.

111. Sonic knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and Class members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

112. As a direct and proximate result of Sonic's violation of the ICFA, Plaintiff and Class members suffered injuries including, but not limited to: (i) damages arising from the unauthorized charges on debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Class Members; (ii) damages arising from Plaintiff's and the Class' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach (including but not limited to late fees and foregone cash back rewards); (iii) damages from time spent and effort expended to mitigate the actual and potential impact of the Data Breach 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; and (iv) damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The

nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

113. Also as a direct result of Sonic's knowing violation of the ICFA, Plaintiff and Class members are entitled to damages as well as injunctive relief, including, but not limited to:

a. Ordering that Sonic engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Sonic's systems on a periodic basis, and ordering Sonic to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Sonic engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Sonic audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Sonic segment PII by, among other things, creating firewalls and access controls so that if one area of Sonic is compromised, hackers cannot gain access to other portions of Sonic systems;

e. Ordering that Sonic purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Sonic conduct regular database scanning and securing checks;

g. Ordering that Sonic routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Sonic to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Sonic customers must take to protect themselves.

114. Plaintiff brings this action on behalf of herself and Class Members for the relief requested above and to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and Class members and the public from Sonic's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Sonic's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

115. Plaintiff and Class members are entitled to a judgment against Sonic for actual and consequential damages, exemplary damages and attorneys' fees pursuant to the ICFA, costs, and such other further relief as the Court deems just and proper.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Sonic as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiff and her Counsel to represent the Nationwide Class or, in the alternative, the separate Statewide Class;

b. For equitable relief enjoining Sonic from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' PII, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiff and Class members;

c. For equitable relief compelling Sonic to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to class members the type of PII compromised;

d. For an award of damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

Dated: December 17, 2017

Respectfully submitted,

By: /s/ Kasif Khowaja

Kasif Khowaja
Frank Castiglione
THE KHOWAJA LAW FIRM, LLC
70 East Lake Street Suite 1220
Chicago, IL 60601
Telephone: (312) 356-3200
Email: kasif@khowajalaw.com
fcastiglione@khowajalaw.com

Brian P. Murray (*pro hac vice*)
Bryan G. Faubus (*pro hac vice*)
GLANCY PRONGAY & MURRAY LLP
230 Park Ave Suite 530
New York, New York 10169
Telephone: (212) 682-5340
Facsimile: (212) 884-0988
Email: bmurray@glancylaw.com
bfaubus@glancylaw.com

Paul C. Whalen
LAW OFFICE OF PAUL C. WHALEN, P.C.
768 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870
Email: pcwhalen@gmail.com

Jasper D. Ward IV
JONES WARD PLC
312 S. Fourth Street
Louisville, KY 40202
Telephone: (502) 882-6000
Email: jasper@jonesward.com

John Yanchunis
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 275-5272
Email: jyanchunis@forthepeople.com

Jean S. Martin
LAW OFFICE OF JEAN SUTTON MARTIN PLLC
2018 Eastwood Road. Suite 225
Wilmington, NC 28403
Telephone: (800) 678-6612
Email: jean@jsmlawoffice.com

Attorneys for Plaintiff

ILND 44 (Rev. 07/10/17)

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

CLARA HUGHES-HILLMAN, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff **Cook County, IL**
(Except in U.S. plaintiff cases)

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

See Attachment

DEFENDANTS

SONIC CORPORATION

County of Residence of First Listed Defendant **Oklahoma County, OK**
(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
- ☐ 365 Personal Injury - Product Liability
- ☐ 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

Habeas Corpus:
- ☐ 530 General
- ☐ 535 Death Penalty
- ☐ 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
- ☐ 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 Immigrant 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)(2) - Negligence

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 $ **$5,000,000**

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

12/17/2017

Signature of attorney of record

/s/ Kasif Khowaja

Attachment to Civil Cover Sheet

Response to (1.)(c.)

Brian P. Murray (*pro hac vice*) Bryan G. Faubus (*pro hac vice*) **GLANCY PRONGAY & MURRAY LLP** 230 Park Ave Suite 530 New York, New York 10169 Telephone: (212) 682-5340 Facsimile: (212) 884-0988 Email: bmurray@glancylaw.com bfaubus@glancylaw.com	Kasif Khowaja Frank Castiglione **THE KHOWAJA LAW FIRM, LLC** 70 East Lake Street Suite 1220 Chicago, IL 60601 Telephone: (312) 356-3200 Email: kasif@khowajalaw.com fcastiglione@khowajalaw.com
Paul C. Whalen **LAW OFFICE OF PAUL C. WHALEN** 768 Plandome Road Manhasset, NY 11030 Telephone: (516) 426-6870 Email: pcwhalen@gmail.com	Jasper D. Ward IV **JONES WARD PLC** 312 S. Fourth Street Louisville, KY 40202 Telephone: (502) 882-6000 Email: jasper@jonesward.com
John Yanchunis **MORGAN & MORGAN COMPLEX LITIGATION GROUP** 201 North Franklin Street, 7th Floor Tampa, Florida 33602 Telephone: (813) 275-5272 Email: jyanchunis@forthepeople.com	Jean S. Martin **LAW OFFICE OF JEAN SUTTON MARTIN PLLC** 2018 Eastwood Road. Suite 225 Wilmington, NC 28403 Telephone: (800) 678-6612 Email: jean@jsmlawoffice.com