IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

GARY ROWE, *individually and on behalf of all others similarly situated,*	**Case No.**
Plaintiff,	**Judge**
v.	**Magistrate Judge**
PARKER HANNIFIN CORPORATION,	**CLASS ACTION COMPLAINT**
Defendant.	**JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Gary Rowe, individually and on behalf of all others similarly situated, brings this this Class Action Complaint ("Complaint") against Defendant Parker Hannifin Corporation ("Parker" or "Defendant"), an Ohio corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") involving Parker Hannifin, a multibillion-dollar manufacturing company headquartered in Cleveland, Ohio.

2. Parker Hannifin failed to properly safeguard its current and former employees' (and their dependents') personally identifiable information ("PII"), including but not limited to their full names, Social Security numbers, dates of birth, addresses, driver's license numbers, U.S. passport numbers, financial account information (bank account and routing numbers), online account usernames, and passwords, as well as protected health information ("PHI"), including but

not limited to enrollment information (such as health insurance plan member ID numbers), dates of coverage, dates of service, provider names, claims information, and medical and clinical treatment information (PII and PHI are referred to collectively as "Private Information").

3. As a result of Defendant's failures, Plaintiff and thousands of other individuals ("Class Members") have had their most sensitive personal information stolen and publicly published on the internet. The information that was published to the internet is one-stop shopping for identity thieves to wreak complete havoc on their victims' lives. Moreover, given the sensitivity and static nature of the information involved (such as names, Social Security numbers, dates of birth), Plaintiff and Class Members will be forced to live in fear forever.

4. Businesses that collect and store Private Information about their employees and employees' families have statutory, regulatory, contractual, and common law duties to safeguard that information and ensure it remains private.

5. Plaintiff and those similarly situated relied upon Defendant to maintain the security and privacy of the Private Information entrusted to it as part of the condition of employment. Plaintiff and Class Members reasonably expected and understood that Defendant would comply with its obligations to keep the Private Information secure and safe from unauthorized access, and to delete Private Information that was not reasonably necessary to hold for a legitimate business purpose.

6. Defendant is responsible for allowing this data breach through its failure to implement and maintain reasonable network safeguards, its unreasonable data retention policies, failure to adequately train employees, and its failure to comply with industry-standard data security practices.

7. Plaintiffs and members of the proposed Class have suffered actual and imminent

injuries as a direct result of the data breach. The actual and imminent injuries suffered by Plaintiffs and the proposed Class as a direct result of the data breach include: (a) theft of their personal data; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to monitor, ameliorate, mitigate and deal with the consequences of the data breach (d) the anxiety, stress, nuisance, and annoyance of dealing with all issues resulting from the data breach; (e) actual fraudulent activity on financial accounts (f) increased fraudulent robo calls and phishing email attempts (g) the potential for future fraud and the increased risk of identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (h) damages to and diminution in value of their personal data entrusted to Defendant; (i) the retention of the reasonable value of the Private Information entrusted to Defendant; and (j) the continued risk to their personal data which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its possession.

8. Accordingly, Plaintiffs, on behalf of themselves and other members of the Class (as defined *infra*), assert claims for negligence, breach of implied contract, and unjust enrichment, and seek injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Plaintiff Rowe

9. Plaintiff is a natural person and a resident and citizen of Southington, Connecticut.

Defendant Parker Hannifin

10. Defendant is a publicly traded corporation incorporated in the State of Ohio and headquartered in Cleveland, Ohio. All of Plaintiff's claims stated herein are asserted against

Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION & VENUE

11. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

12. The Northern District of Ohio has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Ohio and this District through its headquarters, offices, parents, and affiliates.

13. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Background

14. Parker Hannifin is a Fortune 250 engineering company specializing in motion and control technologies, with corporate headquarters in Mayfield Heights, Ohio, in Greater Cleveland. The company provides precision engineered solutions for organizations in the aerospace, mobile, and industrial sectors. It has thousands of employees.

15. In applying for jobs and/or accepting employment with Defendant, Plaintiff and Class Members were required to provide Defendant with sensitive and confidential information, including their names, dates of birth, and Social Security numbers, which is static information that

does not change and can be used to commit myriad financial crimes. Applicants must also provide additional information, including but not limited to health information, financial account information, and government issued identification numbers.

16. Plaintiff and Class Members relied on Defendant (a large, sophisticated entity) to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

17. Defendant had a duty to take reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. This duty is inherent in the nature of the exchange of highly sensitive personal information. Defendant also recognized and voluntarily adopted additional duties to protect Private Information in its Personal Data Privacy Policy ("Privacy Policy"), which has been publicly posted to the internet and is, upon information and belief, provided directly to its employees.[1]

18. The purpose of this policy is to "inform employees and third parties with whom Parker has a business relationship of the principles under which Parker collects, uses, transfers and retains Personal Data" and "applies to all Personal Data received or collected by Parker."[2]

19. The Privacy Policy includes the following representations:

> Only the Personal Data that is necessary for a legitimate business reason or as required by applicable laws or regulations (the "Purpose") should be collected and Processed. When the Purpose for the Personal Data has ended or is no longer relevant, the Personal Data should be deleted, taking into consideration the relevant Records Retention and Protection Guidelines (1.04). Any retention of Personal Data beyond the relevant time period set forth in the Records Retention and Protection Guidelines (1.04) must be documented and explicitly state the reasoning for such retention beyond the specified period.
> …
> Parker collects and uses Personal Data for the purposes of management and

[1] *See* https://www.parker.com/portal/site/PARKER/menuitem.4450f18f18c082cdfd40eae8237ad1ca/?vgnextoid=cb333a5693983610VgnVCM100000e6651dacRCRD (last visited May 19, 2022).
[2] *Id.*

> administration of its pre-employment, employment, and post-employment relationships. The Personal Data is collected and used for hiring activities, general workforce management (described further below), administering security at Parker facilities and on Parker information systems, and as necessary to maintain Parker's third party relationships with customers, suppliers, and other third parties. General workforce management includes, for example, time and attendance tracking, payroll, brokering, providing and administering services and other benefits to employees and their dependents and beneficiaries, job performance and talent management, production of company address books and directories, management of communication systems, training and employee development, providing and monitoring the use of company resources such as company vehicles, mobile phones, computers, and travel and mobility services, managing emergency contact details, and meeting governmental reporting requirements.
>
> …
>
> Parker also may transfer Personal Data between countries, including but not limited to Parker's global headquarters located in the United States of America. Parker is committed to protecting the privacy and confidentiality of Personal Data when it is transferred and employs adequate safeguards and protections in any such transfer, including compliance with the EU-US (and the Swiss-US) Privacy Shield Framework.
>
> …
>
> Parker takes reasonable precautions to protect Personal Data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. These precautions include, for example, password protections for online information systems, restricting access to Personal Data, and employing electronic security measures to protect against hacking or other unauthorized access. Additionally, Parker provides physical security to prevent unauthorized access to database equipment or hard copies of Personal Data.

The Data Breach

20. On January 21, 2021, Defendant detected suspicious activity on its network.

21. Between March 11 and March 14, 2022, a third party gained unauthorized access to Defendant's computer systems and exfiltrated 419GB worth of documents containing the sensitive information of its current and former employees.[3]

22. On April 1, 2022, the well-known ransomware group named Conti took credit for the Data Breach and posted a 5GB sample of stolen data to the internet.

[3] https://www.bleepingcomputer.com/news/security/engineering-firm-parker-discloses-data-breach-after-ransomware-attack/amp/ (last visited May 19, 2022).

23. The Private Information Conti exfiltrated in the Data Breach was held in unencrypted form by Defendant.

24. Incredibly, Defendant continued to possess Plaintiff's and Class Members' Private Information for many years including up to several decades for some Class Members regardless of whether they remained employed with Defendant. There is no reasonable justification for Defendant to retain Plaintiffs' and Class Members' Private Information in unencrypted form for such long periods of time.

25. Upon information and belief, Conti demanded that Defendant pay a ransom for the safe return and deletion of the Private Information stolen from it. Upon information and belief, Defendant refused this demand.

26. On April 20, 2022, Conti published the entire 419GB data set stolen from Defendant to the internet.

27. Cybersecurity experts have specifically noted that the information taken in the Data Breach "would make it possible for malicious actors to carry out phishing attacks, social engineering, or even identity theft and bank fraud."[4]

28. Despite the incredible risk faced by Plaintiff and Class Members, Defendant waited until May 12, 2022 to begin mailing notification letters to the victims of the Data Breach.

29. Defendant's notification letters to victims of the Data Breach reprehensibly downplayed the risk victims face by failing to mention that their most sensitive Private Information had already been published to the internet.

30. On May 13, 2022, Defendant notified the U.S. Department of Health and Human Services Office for Civil Rights ("HHS OCR") that the Data Breach included the Private

[4] https://www.bleepingcomputer.com/news/security/engineering-firm-parker-discloses-data-breach-after-ransomware-attack/amp/ (last visited May 19, 2022).

Information of 119,513 current and former employees.[5] Upon information and belief, the number of victims is greater than this, as it has been reported that the number publicly posted on the HHS OCR website only includes individuals currently or formerly enrolled in the Parker Group Health Plan.[6]

31. Defendant has tacitly admitted that the Private Information stolen and subsequently published to the internet was unencrypted. California law requires companies to notify California residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1). Defendant notified the California Attorney General of the Data Breach on or about May 12, 2021, evidencing that the exposed data was unencrypted.[7]

Securing PII and Preventing Breaches

32. Defendant could have prevented this Data Breach by properly securing and encrypting the Private Information of Plaintiff and Class Members, by properly training its employees recognize and prevent cybersecurity risks, and/or by destroying the data it no longer needed.

33. "In September 2021, the US Cybersecurity and Infrastructure Security Agency (CISA) and the US Federal Bureau of Investigation (FBI) reported that more than 400 Conti ransomware attacks had taken place on U.S. and international organizations. Conti actors frequently use a double extortion tactic: if the victim refuses to pay for data decryption, the malicious actor threatens to leak the data or sell it for profit."[8]

---

[5] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited May 19, 2022).
[6] https://www.hipaajournal.com/parker-hannifin-cyberattack-affects-almost-120000-health-plan-members/ (May 19, 2022).
[7] https://oag.ca.gov/privacy/databreach/list (last visited May 19, 2022).
[8] https://www.cybereason.com/blog/threat-analysis-report-from-shatak-emails-to-the-conti-ransomware (last visited May 19, 2022).

34. Defendant, a multibillion-dollar corporation with sensitive government defense contracts and troves of sensitive employee information, either knew or should have known, and should have taken steps to prevent, Conti's widely publicized methods of attack.

35. The specifics of Conti's attack practices are well documented. Public reports by cybersecurity firms, such as a November 11, 2022 threat analysis report from the Cybereason Global SOC Team, walk readers step by step through Conti's methods of attack and how such attacks can be prevented.[9]

36. Despite the sophistication of Conti and its ransomware, it must still rely on rudimentary tactics for deploying malware on data rich systems, such as basic phishing emails.[10] Such attacks are entirely preventable through proper training of employees to recognize phishing emails in combination with industry standard security measures such as required two-factor or multi-factor authentication to access email accounts and/or other computer systems.

37. Even with a successful initial infection vector through basic phishing techniques, Conti ransomware attacks may be identified and prevented by widely available software, such as the Cyberreason Defense Platform, which is known to "fully detect[] and prevent[] the Conti ransomware."[11]

38. Despite the well-known risks, Defendant inexplicably failed to properly train employees, failed to implement industry standard security measures, and maintained highly sensitive employee information in a manner it knew or should have known was vulnerable to access and exfiltration.

---

[9] https://www.cybereason.com/blog/threat-analysis-report-from-shatak-emails-to-the-conti-ransomware (last visited May 19, 2022).
[10] https://www.cybereason.com/blog/research/cybereason-vs.-conti-ransomware (last visited May 19, 2022).
[11] https://www.cybereason.com/blog/research/cybereason-vs.-conti-ransomware (last visited May 19, 2022).

Value of Personal Identifiable Information

39. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[13] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

40. Social Security numbers, for example, 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. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[14]

41. It is incredibly difficult to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and

---

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 17, 2022).

[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 17, 2022).

[14] *Identity Theft and Your Social Security Number*, Social Security Administration, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 13, 2021).

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.

42. 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 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."[15]

43. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, only credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach, including Social Security number and name, is impossible to "close" and difficult, if not impossible, to change.

44. This data 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."[16]

45. 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.

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

---

[15] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 17, 2022).

[16] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 17, 2022).

47. 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.[17]

48. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

49. 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.

50. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's storage platform, amounting to potentially tens or hundreds of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

51. To date, Defendant has offered Plaintiff and Class Members only two years of identity theft detection services. The offered service is wholly inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the Private

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Jan. 17, 2022).

Information at issue here.

52. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff's Experience

53. Plaintiff Rowe received a letter from Parker dated May 10, 2022 stating that it had determined an unauthorized actor gained access to files on its system that may have contained Plaintiff's name, Social Security number, date of birth, address, driver's license number. U.S. passport number, financial account information (bank account and routing numbers), and online account username/password. The letter further states that if Plaintiff is a current or former member of Parker's Group Health Plan (or a health plan sponsored by an entity acquired by Parker), the incident may have also resulted in unauthorized access to files that additionally contain his enrollment information, including health insurance plan member ID number and dates of coverage.

54. As a result of the Data Breach, Plaintiff Rowe made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Rowe has spent several hours dealing with the Data Breach, valuable time Plaintiff Rowe otherwise would have spent on other activities, including but not limited to work and/or recreation.

55. As a result of the Data Breach, Plaintiff Rowe has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using

his Private Information for purposes of identity theft and fraud. Plaintiff Rowe is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

56. Plaintiff Rowe suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Rowe; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

57. As a result of the Data Breach, Plaintiff Rowe anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Rowe is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ACTION ALLEGATIONS

58. Plaintiff brings this nationwide class action on behalf of himself and all others similarly situated under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

59. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> **All persons Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

60. Excluded from the Class are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

61. Plaintiff reserves the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

62. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of more than 100,000 current and former employees of Defendant whose sensitive data was compromised in Data Breach.

63. Commonality. 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 Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant breached a fiduciary duty to Plaintiffs and Class Members;

m. Whether Defendant violated the consumer protection statute invoked below;

n. Whether Defendant breach implied or express contracts with Plaintiffs and Class Members;

o. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

p. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

q. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

64. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

65. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating Class actions.

66. Predominance. Defendant have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

67. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

68. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

COUNT I
Negligence
(on behalf of Plaintiff and the Class)

69. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

70. As a condition of applying for jobs and/or maintaining employment with Defendant, Plaintiff and the Class were obligated to provide Defendant with their Private Information.

71. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would exercise reasonable care in the protection of their Private Information.

72. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

73. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class.

74. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, configuring, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

75. Defendant also had a duty to exercise appropriate clearinghouse practices to remove job applicants' Private Information it was no longer required to retain pursuant to regulations.

76. Defendant had a duty to properly train employees to recognize phishing attempts and other common data security risks.

77. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Nationwide Class.

78. Defendant's duty to use reasonable security measures arose as a result of the relationship that existed between Defendant and Plaintiff and the Nationwide Class. That relationship arose because Plaintiff and the Nationwide Class entrusted Defendant with their confidential Private Information, a necessary part of applying for jobs and/or maintaining employment with Defendant.

79. Defendant was subject to an independent duty untethered to any contract between Defendant and Plaintiff or the Class.

80. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

81. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information.

82. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to encrypt the data stored on its system or to implement other reasonable industry standard measures to safeguard Private Information.

83. Plaintiff and the Class had no ability to protect their Private Information that was in, and remains in, Defendant's possession.

84. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

85. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

86. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

87. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

88. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

89. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of job applicants' Private Information.

90. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove job applicants' Private Information it was no longer required to retain pursuant to regulations.

91. Defendant breached its duty to adequately train employees to recognize and avoid phishing attempts and other basic cybersecurity risks.

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

93. Defendant breached its duty to safeguard Plaintiff's and Class Members' Private Information by failing to retain such information in an encrypted form.

94. Defendant breached its duty to safeguard Plaintiff's and Class Members' Private Information by retaining the information for many years including for several decades regardless of whether the current or former employee remained employed with Defendant.

95. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Private Information of Plaintiff and the Class would not have been compromised.

96. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

97. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

98. As a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

99. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further

unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

100. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
Breach of Implied Contract
(on behalf of Plaintiff and the Class)

101. Plaintiff re-alleges and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

102. Defendant required Plaintiff and the Nationwide Class to provide their Private Information as a condition of applying for and/or maintaining employment. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

103. Defendant further entered into an implied contract with Plaintiff and the Class to honor the representations discussed *infra* in its Privacy Policy.

104. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

105. Defendant breached the implied contracts it made with Plaintiff and the Class by (i) failing to implement technical, administrative, and physical security measures to protect the Private Information from unauthorized access or disclosure and improper (such as encryption of Social Security numbers) despite such measures being readily available, (ii) failing to limit access to the Private Information to Defendant's employees who needed such information to perform a

specific job, (iii) failing to store the Private Information only on servers kept in a secure, restricted access area, and (iv) otherwise failing to safeguard the Private Information.

106. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

107. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Unjust Enrichment
(on behalf of Plaintiff and the Class)

108. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

109. This claim is brought in the alternative to Plaintiff's claim for breach of implied contract.

110. Defendant benefited from receiving Plaintiff's and Class Members' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

111. Defendant also understood and appreciated that Plaintiff's and Class Members' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

112. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of providing an ability to find people to employ, and in connection thereto, by providing their Private Information to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received adequate protection and data security for such Private Information held by Defendant.

113. Defendant knew Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

114. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiff and Class Members.

115. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures mandated by industry standard.

116. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

117. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

118. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and his counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: May 23, 2022 Respectfully Submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579)
Dylan J. Gould (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Gary M. Klinger (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
221 West Monroe Street, Suite 2100
Chicago, IL 60606
(847) 208-4585
gklinger@milberg.com

David K. Lietz (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20115
(866) 252-0878
dlietz@milberg.com

Attorneys for Plaintiffs and the Proposed Class