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

MICHELLE MULANAX, individually, and on behalf of all others similarly situated, 704 Tinkers Lane Northfield, OH 44067-2306	Case No.: Judge
Plaintiff,	**CLASS ACTION COMPLAINT**
v.	**JURY TRIAL DEMANDED**
PARKER-HANNIFIN CORPORATION % Nicholas Strieker, Registered Agent 4495 West 140th Street Cleveland, OH 44135	
Defendant.	

CLASS ACTION COMPLAINT

Plaintiff Michelle Mulanax, individually, and on behalf of all others similarly situated ("Plaintiff"), by and through her attorneys, brings this action against Defendant Parker-Hannifin Corporation ("Defendant"), and alleges upon personal knowledge as to her own actions and experiences, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This consumer data breach arises out of Defendant's unreasonable, unlawful, and unfair practices with regard to its collection and maintenance of the highly sensitive and confidential personal, financial, and health care information of its current and former employees. Defendant's insufficient and unreasonable data security practices caused, facilitated, and exacerbated the data breach (the "Data Breach") and its impact on Plaintiff and Class members. By Defendant's own admission, the Data Breach went undetected for a four day period from March

11, 2022 through March 14, 2022, and exposed its current and former employees'—including Plaintiff—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 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").

2. Defendant is a Fortune 250 global leader in motion and control technologies headquartered in Cleveland, Ohio.[1]

3. The Private Information that Defendant compromised, exposed, and criminals stole in the Data Breach consists of some of the most sensitive and damaging information when in the hands of criminals, including their names, Social Security numbers, dates of birth, driver's license numbers, U.S. passport numbers, financial account information, online username/password, and health information.

4. The Private Information stolen in the Data Breach can be used by criminals alone, and in conjunction with other pieces of information, to perpetrate crimes against Plaintiff and Class members that can result in significant liability and damage to their money, property, creditworthiness, reputation, and their ability to pay current loans, improve their credit, and/or obtain loans on favorable terms in the future.

[1] https://www.parker.com/portal/site/PARKER/menuitem.c17ed99692643c6315731910237ad1ca/?vgnextoid=a80b0ce599a5e210VgnVCM10000048021dacRCRD&vgnextfmt=EN (last visited May 26, 2022).

5. 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.

6. 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 safe and secure from unauthorized access, and to delete Private Information that was not reasonably necessary to hold for a legitimate business purpose.

7. 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.

8. Plaintiff and the Class have suffered actual and imminent injuries as a direct result of the data breach. The actual and imminent injuries suffered by Plaintiff and the 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.

9. Accordingly, Plaintiff, on behalf of herself and other members of the Class (as defined infra), asserts claims for negligence, breach of implied contract, and unjust enrichment, and seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

PARTIES

10. Plaintiff Michelle Mulanax is a natural person and a citizen of Ohio, and resident of Cuyahoga County, Ohio.

11. Defendant Parker-Hannifin Corporation is a publicly traded corporation incorporated under the laws of the State of Ohio and headquartered in Cleveland, Ohio.

JURISDICTION AND VENUE

12. 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.

13. 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.

14. 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.

NATURE OF THE ACTION

15. Defendant 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.

16. 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.

17. 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.

18. 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.[2]

19. 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."[3]

THE DATA BREACH

20. Between March 11, 2022 and March 14, 2022, a third party gained access to Defendant's computer systems and exfiltrated 419 GB worth of documents containing the Private Information of Defendant's current and former employees.[4]

21. On April 1, 2022, Conti—a ransomware group—claimed responsibility and posted 3% of the data they stole during the Data Breach.[5]

22. On April 20, 2022, Conti published the entire data set online.[6]

23. Defendant continued to possess Plaintiff's and Class members' Private Information for many years—including holding Plaintiff's Private Information for over 10 years after she last worked for the Defendant—regardless of whether they remained employed with Defendant. There is no reasonable justification for Defendant to retain Plaintiff's and Class members' Private Information in unencrypted form for such long periods of time.

24. 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

---

[2] https://parkerstoretest.parker.com/portal/site/PARKER/menuitem.4450f18f18c082cdfd40eae8237ad1ca/?vgnextoid=760b904cf58b2110VgnVCM100000c9040d0aRCRD&vgnextfmt=default (last visited May 26, 2022)

[3] *Id.*

[4] https://www.bleepingcomputer.com/news/security/engineering-firm-parker-discloses-data-breach-after-ransomware-attack/ (last visited May 26, 2022)

[5] *Id*. (last visited May 26, 2022)

[6] *Id*. (last visited May 26, 2022)

engineering, or even identity theft and bank fraud.[7]

25. Defendant waited until May 10, 2022 to begin mailing notification letters to victims of the Date Breach. *See* Defendant's Data Breach Notification Letter, attached hereto as Exhibit 1 (the "Breach Letter").

26. Defendant's Breach Letter failed to notify Plaintiff and Class members that Conti had published the Private Information on the internet. *See* Exhibit 1.

27. On May 13, 2022, Defendant notified the U.S. Department of Health and Human Services Office for Civil Rights that the Data Breach included the Private Information of 119,513 current and former employees.[8]

28. 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, 2022, evidencing that the exposed data was unencrypted.[9]

CYBER SECURITY AND RANSOMWARE ATTACKS ARE FORESEEABLE

29. According to the United States Cybersecurity & Infrastructure Security Agency:

> Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

[7] *Id*. (last visited May 26, 2022)
[8] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited May 26, 2022)
[9] https://oag.ca.gov/privacy/databreach/list (last visited May 19, 2022)

https://www.cisa.gov/ransomware (last visited Apr. 16, 2021).

30. Plaintiff's and Class members' Private Information was stored on files that were exposed in the Data Breach.

31. This situation presents the certainly impending possibility that the hackers will attempt to exert whatever leverage they have to obtain payment.

32. Defendant failed to implement reasonable industry standards necessary to prevent a data breach in compliance with the FTC's guidelines.

33. Defendant failed to create, maintain, and/or comply with a written cybersecurity program that incorporated physical, technical, and administrative safeguards for the protection of its customers' personal information in compliance with industry recognized cybersecurity framework.

34. Because of its failure to create, maintain, and/or comply with a necessary cybersecurity program, Defendant was unable to ensure the protection of information security and confidentiality, and unable to protect against obvious and readily foreseeable threats to information security and confidentiality or the unauthorized access to Plaintiff's and Class members' Personal Information.

PLAINTIFF AND CLASS MEMBERS ARE AT INCREASED RISK OF IDENTITY THEFT

35. As observed in the Trend Micro analysis of the Doppel Paymer ransomware, the ransomware is not employed until the hacker has gained access to high value information and systems. Once the hackers have secretly searched the system to their satisfaction, they execute the ransomware, which encrypts what are believed to be the most sensitive or valuable files. As a result, Plaintiff and Class members have the reasonable belief that their personal, medical and

financial information is now in the hands of hackers that will or already have misused their data or sold it to other criminals who have or will do so in the future.

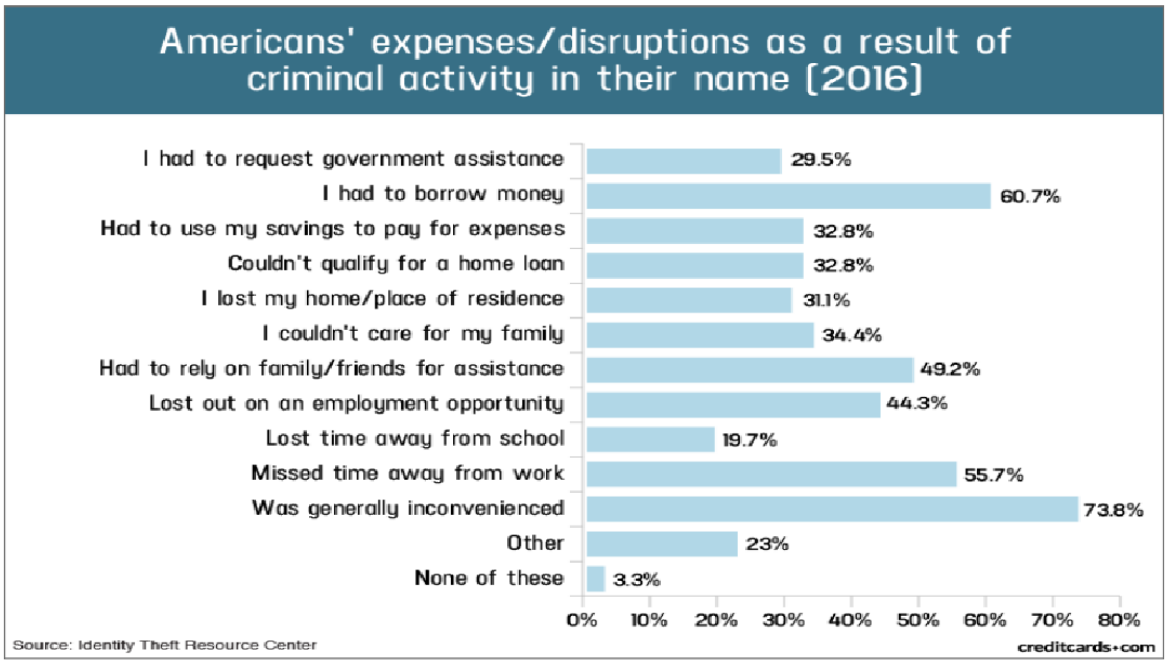
36. The FTC recommends that identity theft victims take several steps to protect their personal, financial, and healthcare information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if they learn someone has abused their information), reviewing their credit reports, contacting companies to dispute fraudulent charges on accounts, placing a credit freeze on their credit, and correcting their credit reports.[10]

37. Identity thieves use another's personal information, such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

38. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's photograph, use the victim's name and Social Security number to obtain government benefits, or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

39. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal, financial, and healthcare information:

[10] *See* https://www.identitytheft.gov/Steps (last visited Apr. 19, 2021)



Source: "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/17, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Apr. 19, 2021).

40. According to the Electronic Privacy Information Center:

> Identity theft is an enormous problem for consumers. The Federal Trade Commission reported 399, 225 cases of identity theft in the United States in 2016. Of that number, 29% involved the use of personal data to commit tax fraud. More than 32% reported that their data was used to commit credit card fraud, up sharply from 16% in 2015. A 2015 report from the Department of Justice found that 86% of the victims of identity theft experienced the fraudulent use of existing account information, such as credit card or bank account information. The same report estimated the cost to the U.S. economy at $15.4 billion.

41. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, or are yet to be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the

future.[11]

THE DATA BREACH WAS PREVENTABLE

42. Data breaches are preventable.[12] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[13] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[14]

43. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[15]

THE VALUE OF THE PERSONAL IDENTIFYING INFORMATION AND CONFIDENTIAL MEDICAL DATA

44. It is well known that Private Information including Social Security numbers and dates of birth with names and addresses, is a valuable commodity and frequent target of criminal attacks.

45. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[16]

---

[11] https://epic.org/privacy/data-breach/equifax/ (last visited Apr. 19, 2021)
[12] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012)
[13] *Id.* at 17
[14] *Id.* at 28
[15] *Id.*
[16] Javelin Strategy & Research, Identity Fraud Hits All Time High With 16.7 Million US Victims in 2017. According to New Javelin Strategy & Research Study (Feb. 6, 2018),

46. Medical data has particular value on the black market because it often contains all of an individual's PII and PHI, as opposed to a single marker that may be found in a data breach.

47. According to a Trustware report, a healthcare data record may be valued up to $250 per record on the black market compared to $5.40 for the next highest value (a payment card).[17]

FACTS RELATIVE TO PLAINTIFF Mulanax

48. On May 20, 2022, Plaintiff returned from vacation to find in her mail a letter from Defendant dated May 10, 2022. *See* Exhibit 1.

49. The Breach Letter informed Plaintiff that Defendant 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 Defendant's Group Health Plan (or a health plan sponsored by an entity acquired by Defendant), the incident may have also resulted in unauthorized access to files that additionally contain Plaintiff's enrollment information, including her health insurance plan member ID number, and dates of coverage. *See* Exhibit 1.

50. Plaintiff was shocked to receive this letter, as she retired from Defendant as of August 2012, and had no reasonable expectation to believe that Defendant would still have her Private Information.

51. Plaintiff, a former IT Professional with Defendant, was also shocked that the Breach Letter was sent months after Defendant initially discovered the Data Breach.

---

https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin (last visited May 29, 2021)

[17] https://www.securelink.com/blog/healthcare-data-new-prize-hackers (citing https://trustwave.azureedge.net/media/16096/2019-trustwave-global-security-report.pdf?rnd=132056250120000000)

52. Shortly after receiving the Breach Letter, Plaintiff called Defendant's "incident" hotline listed in Exhibit 1 to inquire if Defendant had any further information as to what specific Private Information of Plaintiff had been stolen. During the call a representative of the Defendant indicated Plaintiff's matter would be escalated and as of the date of this Complaint, Plaintiff has yet to receive a call back from Defendant's representatives.

53. Since receiving the Breach Letter, Plaintiff has had to spend time researching her records to try and determine what financial information Defendant may still have had almost a decade later, and reviewing bank statements and her credit reports. In addition to that research Plaintiff has taken the steps of opening a new bank account with a new banking institution, moving all funds into that account as well as changing all direct deposit and auto-pay information. Plaintiff estimates she has had to spend at least eight (8) hours on these actions.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

54. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class members have lost time due to the need to review and monitor financial statements due to the ongoing risk of identity theft.

55. For example, in response to the Data Breach, Plaintiff has spent at least four hours reviewing bank statements for suspicious activity, changing PIN numbers, and adding fraud alerts to their bank accounts.

56. As a result of the Data Breach, Plaintiff and Class members must now be vigilant and review their credit reports for suspected incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

57. Plaintiff and Class members have suffered and will suffer actual injury due to loss

of time and increased risk of identity theft as a direct result of the Data Breach. In addition to fraudulent charges, loss of use of and access to their account funds, costs associated with their inability to obtain money from their accounts, and damage to their credit, Plaintiff and Class members suffered ascertainable losses in the form of out-of-pocket expenses and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

a. Monitoring compromised accounts for fraudulent charges;

b. Canceling and reissuing credit and debit cards linked to the financial information in possession of Defendant;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

g. Placing freezes and alerts with credit reporting agencies;

h. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

i. Contacting their financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be canceled; and

l. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

58. Moreover, Plaintiff and Class members have an interest in ensuring that Defendant

implements reasonable security measures and safeguards to maintain the integrity and confidentiality of their Private Information, including making sure that the storage of data or documents containing personal, financial, and healthcare information is not accessible by unauthorized persons and that access to such data is sufficiently protected.

59. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class members have suffered out-of-pocket losses, anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ALLEGATIONS

60. **Class Definition**: Plaintiff brings this action pursuant to Civ. R. 23, on behalf of a class of similarly situated individuals (the "Class"), defined as follows:

> All persons Defendant identified as being among those individuals impacted by the Data Breach, including all individuals who were sent a Notice of Data Breach whose (1) personally identifiable information was accessed and/or (2) personal healthcare information was accessed by unauthorized third parties.

Excluded from the Class are: (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities' current and former officers and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

61. **Numerosity**: The Class is so numerous that joinder of all members is impracticable. The Class includes more than 100,000 individuals. Class members can easily be identified through Defendant's records, or by other means.

62. **Commonality and Predominance**: There are several questions of law and fact common to the claims of Plaintiff and Class members, which predominate over any individual issue, including:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and/or 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 Plaintiff 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 failed to provide notice of the Data Breach in a timely manner, and

m. Whether Plaintiff and Class members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

63. **Typicality**: Plaintiff's claims are typical of the claims of the other members of the Class. All claims are based on the same legal and factual issues. Plaintiff and each of the Class members provided personal, medical, and financial information to Defendant, and the information was accessed and disseminated for sale by unauthorized hackers. Defendant's conduct was

uniform with respect to all Class members.

64. **Adequacy of Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions. Plaintiff has no interest antagonistic to the Class, and Defendant has no defense unique to Plaintiff.

65. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for members of the Class to prosecute their claims individually. The trial and the litigation of Plaintiff's claims are manageable.

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

66. Plaintiff repeats and realleges the allegations of paragraphs 1 through 65 with the same force and effect as though fully set forth herein.

67. Defendant's actions and inactions were of the type that would result in foreseeable, unreasonable risk of harm to Plaintiff and Class members. Defendant knew, or should have known, of the risks inherent in collecting and storing the personal, financial, and healthcare information of Plaintiff and Class members and the importance of adequate security in storing the information. Additionally, Defendant was well aware of numerous, well-publicized data breaches that exposed the personal, financial, and healthcare information of individuals.

68. Defendant had a common law duty to prevent foreseeable harm to Plaintiff's and Class members' Private Information. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of the failure of Defendant to adopt, implement, and maintain

reasonable security measures so that Plaintiff's and Class members' personal, financial, and healthcare information would not be unsecured and accessible by unauthorized persons.

69. Defendant had a special relationship with Plaintiff and Class members. Defendant was entrusted with Plaintiff's and Class members' personal, financial, and health information and Defendant was in a position to protect the personal, financial, and healthcare information from unauthorized access.

70. The duties of Defendant also arose under section 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect individuals' personal, financial, and healthcare information by companies. Various FTC publications and data security breach orders further form the basis of the duties of Defendant.

71. Defendant had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class members' personal, financial, and healthcare information in its possession so that the personal, financial, and healthcare information would not come within the possession, access, or control of unauthorized persons.

72. More specifically, the duties of Defendant included, among other things, the duty to:

a. Adopt, implement, and maintain adequate security measures for protecting an individual's personal, financial, and healthcare information to ensure that the information is not accessible online by unauthorized persons;

b. Adopt, implement, and maintain adequate security measures for deleting or destroying personal, financial, and healthcare information when Defendant's business needs no longer required such information to be stored and maintained; and

c. Adopt, implement, and maintain processes to quickly detect a data breach and to promptly act on warnings about data breaches, and notify affected persons without unreasonable delay.

73. Defendant breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting an individual's personal, financial, and healthcare information in its possession so that the information would not come within the possession, access, or control of unauthorized persons.

74. Defendant acted with reckless disregard for the security of the personal, financial, and healthcare information of Plaintiff and the Class because Defendant knew or should have known that its data security was not adequate to safeguard the personal, financial, and healthcare information that was collected and stored.

75. Defendant acted with reckless disregard for the rights of Plaintiff and Class members by failing to promptly detect the Data Breach, and further, by failing to notify Plaintiff and Class members of the Data Breach in the most expedient time possible and without unreasonable delay pursuant to common law duties to provide reasonably timely and truthful data-breach notification, so that Plaintiff and Class members could promptly take measures to protect themselves from the consequences of the unauthorized access to the personal, financial, and healthcare information compromised in the Data Breach.

76. As a result of the conduct of Defendant, Plaintiff and Class members have suffered and will continue to suffer foreseeable harm. Plaintiff and Class members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiff and Class members 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.

SECOND CAUSE OF ACTION
Negligence Per Se
(On Behalf of Plaintiff and the Class)

77. Plaintiff repeats and realleges the allegations of paragraphs 1-76 with the same force and effect as though fully set forth herein.

78. "Section 5 of the FTC Act [15 U.S.C. § 45] is a statute that creates enforceable duties, and this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data beach context." *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020). "For example, in *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015), the United States Court of Appeals for the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases." *Capital One Data Security Breach Litigation*, 488 F. Supp. 3d at 407.

79. In addition, Plaintiff and Class members may maintain a negligence per se claim based on conduct declared unlawful under the Safeguards Rule, 16 C.F.R. part 314, promulgated by the FTC pursuant to authority delegated by Congress under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(b), to establish standards for financial institutions relating to administrative, technical, and physical safeguards for nonpublic information, including Plaintiff's and Class members' Private Information.

80. The Safeguards Rule at 16 C.F.R. § 314.4 provides:

> In order to develop, implement, and maintain your information security program, [a financial institution] shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

> (2) Requiring your service providers by contract to implement and maintain such safeguards.
>
> (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

16 C.F.R. § 314.4.

81. The Safeguards Rule is a process-based rule drafted using intentionally broad language and not incorporating any specific information security standard or framework to allow financial institutions flexibility to "shape the information security programs to their particular business and to allow the programs to adapt to changes in technology and threats to the security and integrity of customer information."[18]

82. Defendant was and is a financial institution.

83. Plaintiff's and Class members' Private Information was and is nonpublic personal information and customer information.

84. Defendant committed unlawful acts by failing to comply with the requirements of the Safeguards Rule, including but not limited to, failing to:

a. Upgrade and maintain its data security systems in a meaningful way so as to prevent the Data Breach;

b. Replace email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence ("AI") to detect

[18] Fed. Trade Comm'n, Standards for Safeguarding Customer Information, 84 Fed. Reg. 13158, 13159 (Apr. 4, 2019), also available at https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer- information (last visited Nov. 16, 2021)

and block known and newly introduced malware;

c. Block all inbound and outbound Internet, email, and network traffic to foreign countries;

d. Maintain a secure firewall configuration;

e. Monitor for suspicious or irregular traffic to servers;

f. Monitor for suspicious credentials used to access servers;

g. Monitor for suspicious or irregular activity by known users;

h. Monitor for suspicious or unknown users;

i. Monitor for suspicious or irregular server requests;

j. Monitor for server requests for personal, financial, and healthcare information;

k. Monitor for server requests from VPNs;

l. Monitor for server requests from Tor exit nodes;

m. Identify all connections to the computers where Defendant stores sensitive information;

n. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

o. Scan computers on Defendant's network to identify and profile the operating system and open network services, and disable services that are not needed to prevent hacks or other potential security problems;

p. Pay particular attention to the security of Defendant's web applications—the software used to give information to visitors to its websites and to retrieve information from them;

q. Use a firewall to protect Defendant's computers from hacker attacks while it is connected to a network, especially the Internet;

r. Determine whether a border firewall should be installed where Defendant's network connects to the Internet;

s. Monitor incoming traffic for signs that someone is trying to hack in;

t. Monitor outgoing traffic for signs of a data breach;

u. Identify all connections to the computers where you store sensitive

information;

v. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

w. Not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting its business;

x. Scan computers on its network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

y. Pay particular attention to the security of its web applications—the software used to give information to visitors to its websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

z. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

aa. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

bb. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

cc. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from its system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

85. Plaintiff and Class members are in the group of persons the FTC Act and Safeguards Rule were enacted and implemented to protect, and the harms they suffered in the Data

Breach as a result of Defendant's violations of the FTC Act and Safeguards Rules were the types of harm they designed to prevent.

86. As a result of the conduct of Defendant that violated the FTC Act and the Safeguards Rule, Plaintiff and Class members have suffered and will continue to suffer foreseeable harm. Plaintiff and Class members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiff and Class members 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.

THIRD CAUSE OF ACTION
Invasion of Privacy - Intrusion Upon Seclusion
(On behalf of Plaintiff and the Class)

87. Plaintiff repeats and realleges the allegations of paragraphs 1-86 with the same force and effect as though fully set forth herein.

88. Plaintiff and Class members have objectively reasonable expectations of solitude and seclusion in their personal and private information and the confidentiality of the content of personal information and non-public medical information.

89. Defendant intruded upon that seclusion by allowing the unauthorized access to Plaintiff's and Class members' Private Information without Plaintiff's and Class members' consent, knowledge, authorization, notice, or privilege by negligently maintaining the confidentiality of Plaintiff's and Class members' information as set out above.

90. Defendant's breach of the confidentiality resulted in insecure systems allowing

harmful disclosure of the information to criminals and criminal data markets.

91. The intrusion was offensive and objectionable to Plaintiff, the Class members and to a reasonable person or ordinary sensibilities in that Plaintiff's and Class members' Private Information was disclosed without prior written authorization of Plaintiff and the Class.

92. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and Class members provided and disclosed their Private Information to Defendant privately with the intention that the Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class members were reasonable to believe that such information would be kept private and would not be disclosed without consent. Plaintiff and Class members were further reasonable to believe that the Private Information would be reasonably protected against third party criminal extraction through foreseeable hacking activity.

93. This improper disclosure increased the risk that the personal data was delivered to criminal data markets thereby increasing the risk of identity theft to Plaintiff and Class members.

94. The harm included the erosion of the essential confidential relationship between Plaintiff and Class members and their healthcare providers.

95. As a direct and proximate result of the unauthorized disclosure, Defendant caused Plaintiff and Class members the following damages:

a. Sensitive and confidential information is no longer private;

b. Erosion of provider-patient relationship;

c. Loss of value of provider-patient relationship;

d. General damages for invasion of privacy rights in an amount to be determined by a jury;

e. Nominal damages for each independent violation;

f. Unlawful taking of valuable data without compensating Plaintiff or the Class; and

g. Diminution of value of Plaintiff's and Class members' Private Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Michele Mulanax, individually, and on behalf of all others similarly situated, respectfully requests that judgment be entered in her favor and against Defendant Parker-Hannifin Corporation, as follows:

A. That the Court find that this action satisfies the prerequisites for maintenance as a class action and certifying the Class defined herein;

B. That the Court appoint Plaintiff as the representative of the Class;

C. That the Court appoint Plaintiff's counsel as counsel for the Class;

D. That the Court enter judgment in favor of Plaintiff and the Class against Defendant;

E. That the Court award Plaintiff and Class members actual damages and all other forms of available relief, as applicable;

F. That the Court award Plaintiff and the Class attorney's fees and costs, including interest thereon as allowed or required by law;

G. That the Court enter an injunction requiring Defendant to adopt, implement, and maintain adequate security measures to protect its customers' personal, financial, and healthcare information; and

H. Granting all such further and other relief as the Court deems just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiff Michelle Mulanax, individually, and on behalf of all others similarly situated, hereby demands a trial by jury on all claims so triable.

Respectfully submitted,

/s/ Marc Dann
Marc E. Dann (0039425)
Brian D. Flick (0081605)
Michael Smith(0097147)
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
(216) 373-0539 telephone
(216) 373-0536 facsimile
notices@dannlaw.com

Thomas A. Zimmerman, Jr. (*pro hac vice anticipated*)
tom@attorneyzim.com
Zimmerman Law Offices, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
www.attorneyzim.com
firm@attorneyzim.com

Counsel for Plaintiff and the putative Class