IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

LYNN MCINTOSH, individually and on behalf of all others similarly situated, Plaintiff, v. NAVISTAR, INC., Defendant.	Case No. 21-cv-5810 CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Lynn McIntosh ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through his attorneys, brings this Class Action Complaint against Defendant Navistar, Inc. ("Navistar") and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Navistar for its failure to secure and safeguard his, and approximately 63,000 other individuals', private and confidential personal information, including individuals' names, addresses, dates of birth, Social Security numbers, and information relating to the individuals' participation in the Navistar Health Plan and the Navistar Retiree Health Benefit and Life Insurance Plan, such as information regarding healthcare providers and prescriptions ("PII/PHI").

2. Navistar manufactures trucks, buses, engines, and other products that are used in various industries and has over 12,000 current employees.

3. On or before May 20, 2021, unauthorized individuals gained access to Navistar's IT network and extracted files that contained the PII/PHI of Plaintiff and Class members (the "Data Breach").

4. Navistar owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Navistar breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its employees', former employees', and their dependents' PII/PHI from unauthorized access and disclosure.

5. As a result of Navistar's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all individuals whose PII/PHI was exposed as a result of the Data Breach occurring on or before May 20, 2021, which Navistar learned of on May 20, 2021 and first publicly acknowledged the Data Breach on June 7, 2021.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence *per se*, breach of implied contract, breach of fiduciary duty, and a violation of the Ohio Consumer Sales Practices Act, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

7. Plaintiff Lynn McIntosh is an Ohio resident. He is a former employee of Navistar. He received a letter from Navistar notifying him that his PII/PHI had been exposed in the Data Breach.

8. Defendant Navistar, Inc. is a corporation that is incorporated in Illinois. Defendant's corporate headquarters are located at 2701 Navistar Drive, Lisle, IL 60532.

JURISDICTION AND VENUE

9. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

10. This Court has personal jurisdiction over Navistar because Navistar is a corporation organized under the laws of Illinois.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Navistar's principal place of business is located in Lisle, Illinois.

FACTUAL ALLEGATIONS

12. Navistar is a manufacturer of trucks, buses, engines, and other vehicle parts. Navistar has over 1000 service locations throughout the United States and over 12,000 employees.[1]

13. In the regular course of its business, Navistar collects and maintains the PII/PHI of its employees, former employees, and their dependents and requires its employees to provide the company with their PII/PHI in order to secure employment with the company and to participate in the Navistar Health Plan and the Navistar Retiree Health Benefit and Life Insurance Plan.

14. Plaintiff and Class members are, or were, employees or dependents of those current and former employees of Navistar and entrusted Navistar with their PII/PHI.

[1] *See* Navistar, *Our Company*, *available at* https://www.navistar.com/about-us/our-company (last accessed Oct. 28, 2021)

The Data Breach

15. On or before May 20, 2021, an unauthorized individual, or unauthorized individuals, gained access to Navistar's computer network. It is unclear how long the unauthorized individuals had access to or control over Navistar's computer network.

16. Navistar did not acknowledge that employee PII/PHI was involved in the Data Breach until August 20, 2021, three months after the company discovered the Data Breach. Navistar stated in a press release that the information that was accessed included:

> "full names, addresses, dates of birth, social security numbers, and/or information related to participation in the [Navistar, Inc. Health Plan or the Navistar, Inc. Retiree Health Benefit and Life Insurance Plan]."[2]

17. In the press release, Navistar warns individuals to "remain vigilant" and to "review their account statements and monitor free credit reports."[3]

18. Plaintiff's and all other Class members' information, as well as other information from the Data Breach, was made available for purchase on the dark web.

Navistar Knew that Criminals Target PII/PHI

19. At all relevant times, Navistar knew, or should have known, its employees', former employees', their dependents', Plaintiff's, and all other Class members' PII/PHI was a target for malicious actors. Despite such knowledge, Navistar failed to implement and maintain reasonable and appropriate security measures to protect Plaintiff's and Class members' PII/PHI from cyber-attacks Navistar should have anticipated and guarded against.

---

[2] Navistar, *Notice of Security Incident*, *available at* https://www.navistar.com/security-incident (last accessed Oct. 28, 2021)
[3] *Id*.

20. PII/PHI is a valuable property right.[4] The value of PII/PHI as a commodity is measurable.[5] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[6] American companies are estimated to have spent over $19 Billion on acquiring personal data of consumers in 2018.[7] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

21. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

22. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[8] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten

---

[4] *See* Marc van Lieshout, *The Value of Personal Data*, International Federation for Information Processing (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), *available at* https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data (last accessed Oct. 28, 2021)

[5] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market* (April 28, 2014), *available at* http://www.medscape.com/viewarticle/824192 (last accessed Oct. 28, 2021).

[6] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value* (April 2, 2013), *available at* https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last accessed Oct. 28, 2021)

[7] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, *available at* https://www.iab.com/news/2018-state-of-data-report/ (last accessed Oct. 28, 2021)

[8] *See* Healthtech Magazine, *What Happens to Stolen Healthcare Data*,

personal identifying characteristics of an individual."[9] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[10]

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

23. Theft of PII/PHI is serious. The FTC warns that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[11]

24. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[12] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a

---

https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (Oct. 20, 2019) ("*What Happens to Stolen Healthcare Data* Article") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last accessed Oct. 28, 2021).

[9] *Id.*

[10] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims (last accessed Oct. 28, 2021).

[11] *See* Federal Trade Commission, *What to Know About Identity Theft*, *available at* https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Oct. 28, 2021).

[12] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[13]

25. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[14]

26. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[15]

27. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[16] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[17] In warning individuals on the dangers of

---

[13] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Oct. 28, 2021).

[14] Identity Theft Resource Center, *2021 Consumer Aftermath Report* (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Oct. 6, 2021).

[15] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), *available at* https://time.com/5643643/capital-one-equifax-data-breach-social-security/ (last accessed Oct. 28, 2021).

[16] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft* (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf (last accessed Oct. 28, 2021).

[17] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.13.

medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [18] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[19]

28. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

29. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical identity theft they face and will continue to face.

CLASS ALLEGATIONS

30. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

---

[18] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Oct. 28, 2021).
[19] *Id*.

31. Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

> All individuals whose PHI/PII was accessed by and disclosed to unauthorized persons in the Data Breach, including all who were sent a notice of the Data Breach.

32. Excluded from the Class is Navistar, Inc. and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

33. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

34. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Navistar's notices to state attorneys general regarding the Data Breach stated that the Data Breach affected over 60,000 individuals.

35. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Navistar had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether Navistar failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII/PHI;

c. Whether an implied contract existed between Class members and Navistar providing that Navistar would implement and maintain reasonable security

measures to protect and secure Class Members' PII/PHI from unauthorized access and disclosure;

d. Whether Navistar breached its duties to protect Plaintiff's and Class members' PII/PHI; and

e. Whether Plaintiff and other members of the Class are entitled to damages and the measure of such damages and relief.

36. Navistar engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

37. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts and practices committed by Navistar, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

38. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that he has no interests adverse to, or that conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex class actions of this nature.

39. A class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and other Class members are relatively small compared to the burden and expense that would be

required to individually litigate their claims against Navistar, so it would be impracticable for Class members to individually seek redress from Navistar's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

40. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

41. Navistar owed a duty to Plaintiff and other Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

42. Navistar knew the risks of collecting and storing Plaintiff's and other Class members' PII/PHI and the importance of maintaining secure systems. Navistar knew of the many data breaches that targeted businesses who collected PII/PHI.

43. Given the nature of Navistar's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Navistar should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

44. Navistar breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security

processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

45. It was reasonably foreseeable to Navistar that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

46. But for Navistar's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

47. As a result of Navistar's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

48. Plaintiff's and other Class members' injuries were proximately caused by Navistar's violations of the duties enumerated above, which were conducted with reckless indifference towards the rights of others, such that an award of punitive damages is warranted.

COUNT II

NEGLIGENCE *PER SE*

49. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

50. Navistar's duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Navistar, of failing to employ reasonable measures to protect and secure PII/PHI.

51. Navistar violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and other Class members' PII/PHI and not complying with applicable industry standards. Navistar's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

52. Navistar's violation of Section 5 of the FTCA constitutes negligence *per se*.

53. Plaintiff and Class members are within the class of persons Section 5 of the FTCA was intended to protect.

54. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and other Class members as a result of the Data Brach.

55. It was reasonably foreseeable to Navistar that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt,

implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

56. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Navistar's violation of Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT III

BREACH OF IMPLIED CONTRACT

57. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

58. In connection with their employment and/or their participation in the Navistar Health Plan and the Navistar Retiree Health Benefit and Life Insurance Plan, Plaintiff and other Class members entered into implied contracts with Navistar.

59. Pursuant to these implied contracts, Plaintiff and Class members provided Navistar with their PII/PHI. In exchange, Navistar agreed, among other things, to take reasonable measures to protect the security and confidentiality of Plaintiff's and Class

members' PII/PHI and to protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

60. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Navistar, on the other hand. Had Plaintiff and Class members known that Navistar would not adequately protect their PII/PHI, they would not have provided their PII/PHI to Navistar.

61. Plaintiff and Class members performed their obligations under the implied contract when they provided Navistar with their PII/PHI.

62. Navistar breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

63. Navistar's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach.

64. Plaintiff and other Class members were damaged by Navistar's breach of implied contracts because: (i) they face a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) their PII/PHI was improperly disclosed to unauthorized individuals; (iii) the confidentiality of their PII/PHI has been breached; (iv) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) they have lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT IV

BREACH OF FIDUCIARY DUTY

65. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

66. Plaintiff and Class members gave Navistar their PII/PHI in confidence, believing that Navistar would protect that information. Plaintiff and Class members would not have provided Navistar with this information had they known it would not be adequately protected. Navistar's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between Navistar and Plaintiff and Class members. In light of this relationship, Navistar must act primarily for the benefit of their employees, former employees, and their dependents, which includes safeguarding and protecting Plaintiff's and Class Members' PII/PHI.

67. Navistar has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII/PHI and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected.

68. As a direct and proximate result of Navistar's breaches of its fiduciary duties, Plaintiff and Class members have suffered, and will suffer, injury, including, but not limited to: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII/PHI; (iii) breach of the confidentiality of their PII/PHI; (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate

the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT V

VIOLATION OF THE OHIO CONSUMER SALES PRACTICES ACT ("OCSPA") [O.R.C. Ann. § 1345.01 et seq.]

69. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

70. Navistar offered and continues to offer job applicants employment and an option to participate in the Navistar Health Plan and the Navistar Retiree Health Benefit and Life Insurance Plan.

71. Plaintiff and other Class members provided Navistar with their PII/PHI when they accepted employment with Navistar and/or enrolled in the Navistar Health Plan and the Navistar Retiree Health Benefit and Insurance Plan.

72. Navistar engaged in unlawful and unfair practices in violation of the OCSPA by failing to implement and maintain reasonable security measures to protect and secure its employees', former employees', and their dependents' PII/PHI in a manner that complied with applicable laws, regulations, and industry standards.

73. Due to the Data Breach, Plaintiff and Class members have lost property in the form of their PII/PHI. Further, Navistar's failure to adopt reasonable practices in protecting and safeguarding its employees', former employees', and their dependents' PII/PHI will force Plaintiff and other Class members to spend time or money to protect against identity theft. Plaintiff and Class members are now at a higher risk of identity theft, medical identity theft, and other crimes. This harm sufficiently outweighs any justifications or motives for Navistar's practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

74. Plaintiff and the Class members would not have provided their PII/PHI to Navistar if they had known that Navistar would not apply appropriate and reasonable safeguards to protect their PII/PHI.

75. Plaintiff and other Class members were damaged by Navistar's unlawful and unfair business practices because: (i) they face a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) their PII/PHI was improperly disclosed to unauthorized individuals; (iii) the confidentiality of their PII/PHI has been breached; (iv) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and/or (v) they have lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the other members of the Class, respectfully requests that the Court enter judgment in his favor and against Navistar as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Navistar from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide

or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: October 29, 2021

Respectfully submitted,

/s/ Ben Barnow___

BEN BARNOW
b.barnow@barnowlaw.com
ANTHONY L. PARKHILL
aparkhill@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504