

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION**

DOUG MATTHEWS, individually, and on  
behalf of all others similarly situated,

Plaintiff,

v.

NAVISTAR, INC.,

Defendant.

No.

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiff Doug Matthews (“Plaintiff”), individually and on behalf of all others similarly situated, brings this action against Defendant Navistar, Inc. (“Defendant” or “Navistar”), by and through his attorneys, and alleges as follows based upon personal knowledge as to his own actions, and based upon the investigation of counsel regarding all other matters:

**INTRODUCTION**

1. Best known as the manufacturer and distributor of “International” brand trucks and “IC” brand school and commercial buses, Navistar is one of the largest commercial vehicle manufacturers and service parts distributors in the United States, with a network of more than 1,000 dealers and numerous service partners throughout North America.<sup>1</sup>

2. Defendant currently employs approximately 12,000 workers worldwide, a significant portion of whom are located in the United States. Many of Navistar’s U.S.-based employees are, like Plaintiff, located in Illinois, where Defendant is headquartered and operates both an assembly plant and a parts distribution center.

---

<sup>1</sup> *Our Company*, Navistar, <https://www.navistar.com/about-us/our-company> (last accessed Oct. 20, 2021).

3. In order to secure employment with Navistar, individuals must provide and entrust Defendant with their most sensitive and valuable resource: their personal information, including names, dates of birth, addresses, driver’s license numbers, and Social Security Numbers (“personally identifying information” or “PII”).

4. In order to participate in the Navistar Health Plan and Navistar Retiree Health Benefit and Life Insurance Plan, Navistar also requires employees to provide their PII, as well as information concerning their health care provider, prescriptions, and other protected medical information (“private health information” or “PHI”). If Navistar employees wish to add dependents and/or beneficiaries to either plan—a benefit to which their employment entitles them—those individuals likewise must provide their PII and/or PHI to Navistar.

5. However, despite being one of the nation’s largest vehicle manufacturers and distributors—and employing over the years tens of thousands of individuals who entrusted it with their sensitive and valuable PII and/or PHI—Navistar failed to invest in adequate data security and properly safeguard its information systems. As a direct, proximate and foreseeable result of Navistar’s myriad failures, malevolent actors compromised the highly-sensitive PII and/or PHI of more than 63,000 current and former employees through an eminently avoidable cybersecurity attack.<sup>2</sup>

6. Sometime prior to May 20, 2021, Defendant experienced a data breach through which hackers exfiltrated the PII and PHI of both current and former Navistar employees, including Plaintiff (the “Data Breach”). Critically, many of the categories of PII exposed in the breach, like Social Security Numbers and dates of birth, cannot be changed. Yet, Defendant did

---

<sup>2</sup> *Data Breach Notifications*, Office of the Main Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/1fbf84df-eb26-497d-b138-1a80b7cef361.shtml> (noting that Navistar informed the Maine Attorney General’s Office that the data breach impacted 63,126 individuals) (last visited Oct. 20, 2021).

not disclose the Data Breach to Plaintiff and other affected current and former employees until more than a month after it discovered the Data Breach, and did not disclose the misappropriation of their PHI for several additional months thereafter.

7. Navistar's delays virtually ensured the criminals who exploited Defendant's security failure(s) could monetize, misuse and/or disseminate the PII and PHI Defendant allowed to be misappropriated before Plaintiff and others could take affirmative steps to protect their identities. Now, Plaintiff and similarly situated persons will for years suffer the significant and concrete risk that their identities will be (or already has been) misused—a virtual certainty given that Plaintiff's and the Class' PII and/or PHI were being sold on the dark web long before Navistar notified Class members of the Data Breach.

8. Defendant failed to take adequate and reasonable measures to secure its data systems and all available steps to prevent and stop the Data Breach from occurring; to disclose to current and former employees the material fact that it lacked computer systems and security practices sufficient to safeguard their PII and PHI; and to timely detect and provide adequate notice of the Data Breach. Navistar's failures caused substantial harm and injury to Plaintiff and thousands of other current and former Navistar employees nationwide.

9. As a result of Defendant's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff's and other current and former employees' PII and PHI was accessed and acquired by cybercriminals for the express purpose of misusing the data and causing further irreparable harm to Navistar's current and former employees' personal, financial, reputational, and future well-being. Plaintiff and other current and former Navistar employees face the real, immediate and likely danger of identity theft and the misuse of their PII and PHI, especially because their PII and PHI was specifically targeted

by the hackers. Indeed, news reports indicate this information Defendant allowed to be compromised already has found its way to the dark web, where it may be bought, sold and transferred in perpetuity, causing victims of the Data Breach untold harm.

10. Accordingly, Plaintiff brings this action on behalf of all those similarly situated and against Defendant for its failure to reasonably safeguard Plaintiff's and Class members' PII and PHI, failure to reasonably provide timely notification that Plaintiff's and Class members' PII and PHI had been accessed and acquired by an unauthorized third party, and for intentionally and unconscionably deceiving Plaintiff and Class members concerning the status, safety, location, access, and protection of their PII and PHI.

11. Plaintiff brings claims against Defendant for various statutory violations, as well as negligence, negligence *per se*, bailment, and declaratory judgment.

### **PARTIES**

#### **Plaintiff Doug Matthews**

12. Plaintiff Doug Matthews ("Plaintiff") is a citizen of Illinois, and currently resides in Bellwood, Illinois.

13. Plaintiff currently is employed by Navistar at its Melrose Park, Illinois assembly plant. Plaintiff has been employed by Navistar since 2001. Navistar informed Plaintiff Matthews in January 2021 that it will cease operations at its Melrose Park plant no later than November 24, 2021, and will terminate Plaintiff's employment effective November 29, 2021.

14. In exchange for his employment services, Navistar offered to compensate Plaintiff Matthews and provide him with other employment benefits, including by allowing Plaintiff, his beneficiaries and any dependents to enroll and participate in the Navistar Health Plan and Navistar Retiree Health Benefit and Life Insurance Plan.

15. To receive compensation and employment benefits, however, Navistar required Plaintiff to: (i) provide Navistar with PII to fulfill Navistar's legal responsibilities and operational requirements, including his full name, home address, Social Security Number, telephone number(s) and date of birth, as well as the PII of people designated as beneficiaries on his employment-related benefits through Navistar; (ii) cooperate in providing PHI necessary to determine responsibility for health provider payments; and (iii) provide other confidential information in the course of his employment. Plaintiff believes that all Navistar employees were required to provide the PII, PHI and other confidential information described above as a condition of their employment.

16. Plaintiff accepted Navistar's employment offer and provided the above-referenced categories of highly sensitive information prior to commencing and throughout his employment as Navistar required, with the expectation that Navistar would exercise reasonable care to protect and maintain the confidentiality of his PII, PHI and other confidential information by safeguarding it from compromise, disclosure, and misuse by unauthorized users except to the extent necessary to provide agreed-upon compensation and other employment benefits, and would be timely and forthright relating to any data security incidents involving his and/or his family members' PII and/or PHI.

17. In late July 2021, Plaintiff received from Navistar a letter dated July 6, 2021, and titled "Notice of Data Breach" (the "First Notice"), informing Plaintiff that sometime prior to May 20, 2021, one or more unauthorized persons accessed his PII. Although the letter is dated July 6, Plaintiff did not receive the letter until weeks later, and did not learn of the Data Breach until he received the First Notice.

18. The First Notice stated that on June 16, 2021, Defendant determined that Plaintiff's name, address, and Social Security Number were accessed by the unauthorized actor(s).

19. On or about September 21, 2021, Defendant sent Plaintiff another letter titled "Notice of Data Breach" (the "Second Notice"), informing Plaintiff that on August 20, 2021, Defendant determined that PII and PHI relating to Plaintiff's participation in the Navistar Health Plan or Navistar Retiree Health Benefit and Life Insurance Plan, such as Plaintiff's date of birth, address and information identifying his providers and prescriptions, also was accessed by the unauthorized actor(s) during the Data Breach.

20. On information and belief, additional PII and PHI belonging to Plaintiff was accessed by the hackers in the Data Breach.

21. Although Defendant has known of the Data Breach since at least May 20, 2021, Plaintiff did not learn that his PII had been exfiltrated as a direct and foreseeable result of Defendant's failures until he received the First Notice more than a month after Defendant discovered the Data Breach. Further, Plaintiff did not learn that his PHI had been exfiltrated due to Defendant's failures until he received the Second Notice, months after Defendant first discovered the Data Breach. This delay deprived Plaintiff of the opportunity to take affirmative steps to protect his identity before criminals could further abuse and monetize it.

22. The Data Breach already has required Plaintiff to expend significant time and effort to protect himself and his family from its potential adverse consequences, including but not limited to investigating whether hackers have further attempted to misuse his PII and/or PHI, and potential means by which to protect himself from identity theft, such as by placing fraud alerts on his credit accounts at major credit bureaus, reviewing his credit reports, and monitoring associated bank and credit accounts.

23. Because Plaintiff will be at risk of identity theft indefinitely due to the nature of the PII and PHI Navistar failed to safeguard, Plaintiff ultimately elected to purchase at an initial annual cost of \$419.88<sup>3</sup> Norton 360 with Lifelock Ultimate Plus, a suite of tools designed to, *inter alia*, protect Plaintiff and his family from identity theft. Upon enrolling in Lifelock Ultimate Plus, Lifelock informed Plaintiff that his PII and/or PHI was detected on the dark web, indicating that third-parties either are attempting to or have sold the PII and/or PHI hackers exfiltrated from Navistar's information systems.

24. As a direct, proximate and foreseeable result of the Data Breach, as well as Defendant's failure to prevent against and timely notify Plaintiff of the same, Plaintiff has suffered concrete injuries and damages, including out-of-pocket costs incurred in mitigating the immediate effects of the Data Breach and the heightened risk of fraud and identity theft to which the Breach exposed him.

25. Plaintiff would not have entrusted his PII to Defendant had Defendant disclosed that it lacked computer systems and data security practices sufficient to adequately safeguard the incredibly sensitive PII of Plaintiff and the Class.

**Defendant Navistar**

26. Defendant Navistar, Inc. is a Delaware company headquartered at 2701 Navistar Dr., Lisle, Illinois 60532.

**JURISDICTION AND VENUE**

27. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of \$5,000,000, the number of class members exceeds 100, and Defendant is a

---

<sup>3</sup> Subsequent renewals will cost \$688.99 per year.

citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

28. This Court has personal jurisdiction over Defendant because it is authorized to and regularly conducts business in Illinois, and is headquartered in Lisle, Illinois.

29. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District.

### **GENERAL ALLEGATIONS**

#### ***Navistar, Inc. — Background***

30. Navistar is the manufacturer of “International” brand commercial trucks, diesel engines, and “IC” brand school and commercial buses, as well as a producer and distributor of service parts used to repair trucks and diesel engines. Navistar also provides and manages retail, wholesale, and lease financing of its products. Navistar touts itself as the “industry’s largest service network” with more than 1,000 dealers and Love’s Travel Stop service partners.

31. As of October 2020, Navistar employed approximately 12,000 workers worldwide, including thousands of workers across the United States.

32. As a condition of their employment, Navistar required current and former employees to provide it with highly sensitive PII, including but not limited to their: full name, date of birth, address, telephone number, email address, Social Security Number, and driver’s license number.

33. Current and former employees and their family members are eligible to participate in Navistar’s Health Plan and Navistar’s Retiree Health Benefit and Life Insurance Plan.



Participation in either plan requires the participant to provide certain sensitive and private information, however, including the participant's full name, date of birth, address, and Social Security Number, as well as PHI. Navistar collects, maintains, and has access to the PII and PHI of the participants in the Plans.

34. On information and belief, at the time of the Data Breach Navistar stored and maintained the PII and/or PHI of tens of thousands of current and former employees, as well as their dependents and beneficiaries.

35. Navistar claims to know full well the value and importance of data security. Navistar's operations routinely involve receiving, storing, processing, and transmitting sensitive information pertaining to its business, customers, dealers, suppliers, and employees. As such, Navistar represents that it "continuously seek[s] to maintain a robust program of information security and controls."<sup>4</sup>

36. Current and former employees and their family members provided and made their PII and PHI available to Defendant with the reasonable expectation that Navistar would comply with its obligation to keep their sensitive and personal information, including their PII and PHI, confidential and secure from unauthorized access, and that Defendant would provide them with prompt and accurate notice of any unauthorized access to their PII and/or PHI.

37. Unfortunately for Plaintiff and the Class, Defendant failed to carry out its duty to provide adequate data security, and thus failed to protect current and former employees' PII and PHI, which unauthorized persons exfiltrated during the Data Breach.

---

<sup>4</sup> *Form 10-K* (FY ending Oct. 31, 2020), U.S. Security and Exchange Commission, available at: <https://www.sec.gov/ix?doc=/Archives/edgar/data/808450/000080845020000105/nav10k2020.htm>.

***The Data Breach***

38. On or about June 7, 2021, Navistar disclosed in an 8-K filing to the U.S. Securities and Exchange Commission (“SEC”) that it was affected by a cybersecurity attack: the Data Breach.

39. In the filing, Navistar stated that it on or about May 20, 2021, it learned of a credible potential cybersecurity threat to its information technology system. Defendant began an investigation, and, on or about May 31, 2021, Defendant “received a claim that certain data had been extracted from [its] IT system.”<sup>5</sup> On information and belief, the “claim” that Defendant received on or about May 31, 2021, was a communication from the hackers regarding the Data Breach.

40. Navistar asserts that it began investigating the Data Breach thereafter and determined on or about June 16, 2021, that “some of the data taken by the unauthorized third party contain[ed] personal information about some of [Navistar’s] current and former U.S. employees.”<sup>6</sup>

41. According to Second Notice letters it sent to Plaintiff and the Class in September 2021, on or about August 20, 2021 Navistar also determined that the data exfiltrated by the unauthorized person(s) included information relating to current and former employees’ participation in the Navistar Health Plan and/or Navistar Retiree Health Benefit and Life Insurance Plan, including PII and PHI concerning providers and prescriptions, addresses and birth dates.<sup>7</sup>

42. Navistar has not publicly acknowledged the length of time that unauthorized individuals had access to Navistar’s computer systems, instead stating only that the Data Breach

---

<sup>5</sup> *Form 8-K*, U.S. Securities and Exchange Commission (May 20, 2021), available at: <https://www.sec.gov/ix?doc=/Archives/edgar/data/0000808450/000119312521183688/d13020d8k.htm>

<sup>6</sup> See First Notice, Exhibit A.

<sup>7</sup> See Second Notice, Exhibit B.

occurred prior to May 20, 2021. However, according to some reports the Data Breach “lasted for more than a month.”<sup>8</sup>

43. During the more than a month that the hacker(s) had unrestricted access to Defendant’s computer systems, they were able to access and acquire personal, sensitive, and protected PII and PHI belonging to current and former employees, including but not limited to their names, addresses, dates of birth, Social Security Numbers, driver’s license/state identification numbers, and information relating to their participation in the Health Plan and/or Retiree Health Benefit and Life Insurance Plan, such as the names of medical treatment providers and prescriptions.

***Navistar’s Many Failures Both Prior to and Following the Breach***

44. On or about May 31, 2021, data that was exfiltrated in the Data Breach was posted for sale on Marketo—a “leaked data marketplace.” In the post, the hackers claimed that Navistar “completely ignored [their] warnings[,]”<sup>9</sup> suggesting the hack was part of a ransomware attack. The hackers posted a 315FB “evidence pack” as proof that they were in possession of data from the Data Breach. According to the bid counter on the Marketo website, as of the time of filing 77 individuals have placed bids to purchase the data exfiltrated in the Data Breach.

45. According to the poster(s) on Marketo, instead of preventing the release of its current and former employees’ sensitive, private and personal information, including their PII and PHI, Defendant ignored the hackers (and their likely ransom demands). The hackers then posted the data for sale online. Navistar, in other words, had ample opportunity to safeguard Plaintiff’s and the Class’ data even after its systems were breached, but refused to do so, thereby placing its

---

<sup>8</sup> FreightWaves, *Cyberthieves Say They Have Moral Principles*, Yahoo! (July 21, 2021), available at: <https://www.yahoo.com/now/cyberthieves-moral-principles-144008130.html>

<sup>9</sup> Navistar, Marketo, available at: <https://marketo.cloud/lot/50/?bp=1> (last visited Oct. 20, 2021).

own financial interest above that of the thousands of individuals whose PII and PHI it was duty-bound to protect.

46. Despite learning of the Data Breach on May 20, 2021, and disclosing the Data Breach to the SEC on June 7, 2021, Defendant waited until July to notify current and former employees that Navistar had suffered a Data Breach, and that their PII was accessed and extracted by unauthorized persons. Indeed, although the First Notice letter is dated July 6, Plaintiff and others did not receive the First Notice for weeks thereafter. Moreover, when Defendant finally acknowledged that it had experienced a breach, it failed to inform victims that their PII was made available for sale online more than a month prior.

47. On or about September 21, 2021, Defendant sent the Second Notice to certain victims of the Data Breach. The Second Notice acknowledged that the hackers had accessed additional personal information regarding current and former employees and their family members, including their full names, addresses, dates of birth, Social Security Numbers, and/or information related to their participation in the Navistar health benefit and insurance plans. The Second Notice disclosed that Defendant learned on August 20, 2021, that hackers accessed the current and former employees' PII and PHI. Defendant, in other words, waited a month after learning of the broader scope of the Data Breach—and approximately four (4) months after first discovering the Data Breach—before disclosing the full scope of the Breach to affected individuals.

48. Defendant's failure to properly safeguard Plaintiff's and Class members' PII allowed cybercriminals to access their PII undetected for at least a month, and its failure to promptly notify Plaintiff and other victims of the Data Breach that their PII and PHI had been

misappropriated precluded them from taking meaningful steps to safeguard their identities before their PII and PHI was further disseminated.

49. The length of the Data Breach also demonstrates the inadequacies inherent in Defendant's network monitoring procedures: had Defendant properly monitored its computer systems, it would have discovered the Data Breach much sooner, and likely long before hackers exfiltrated the PII and PHI here at issue.

50. Navistar's lackluster response to the Data Breach has only exacerbated the consequences of its IT failings.

51. First, although Navistar learned of the Data Breach in May 2021, not until late July did it actually notify Plaintiff and the Class that it had allowed their highly-sensitive PII to be stolen, and only in September did it reveal the full scope of the Breach. Further, Navistar has not admitted to Plaintiff and Class members that their PII and PHI was made available for purchase (and likely sold) on the dark web.

52. Second, Navistar's public comments suggest that, despite its myriad security failures, hackers gave it ample opportunity to make amends and protect Plaintiff and the Class' PII and PHI before it was made available for purchase on the dark web. Yet Navistar made no effort to do so, again prioritizing its bottom line over the security of data it was obligated to protect.

53. Third, Navistar has made no effort to protect Plaintiff and the Class from the long-term consequences of Defendant's acts and omissions. Both the First Notice and Second Notice offered a complimentary two year membership in Experian IdentityWorks, but because Class members cannot change their birthdates or Social Security Numbers, malevolent actors can and will continue to misuse this PII for more than a mere two years. Plaintiff and the Class will remain

at a heightened and unreasonable risk of identity theft for years to come, a risk a mere two-years of credit monitoring cannot remedy.

54. In short, Defendant's myriad failures—including to timely detect the Data Breach and to notify Plaintiff and Class members that their PII had been exfiltrated due to Defendant's security failures—allowed cybercriminals to misuse Plaintiff's and Class members' PII and PHI undetected for months before Defendant finally granted them the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

***Data Breaches Pose Significant Threats***

55. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors.

56. In 2018, the Identity Theft Resource Center and CyberScout Annual End-of-Year Data Breach Report revealed a 126% increase in exposed data.<sup>10</sup> Between January and July 2019, more than 31.6 million healthcare records were exposed in data security incidents—more than double the total amount of healthcare data breaches for all of 2018.<sup>11</sup>

57. In fact, Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, estimates that the annual number of data breaches occurring in the United States increased by approximately 692% between 2005 and 2018, a year during which over 446.5 million personal records were exposed due to data breach

---

<sup>10</sup> *2018 End of Year Data Breach Report*, Identity Theft Resource Center, available at: [https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC\\_2018-End-of-Year-Aftermath\\_FINAL\\_V2\\_combinedWEB.pdf](https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf).

<sup>11</sup> Steve Adler, *First Half of 2019 Sees 31.6 Million Healthcare Records Breached*, HIPAA Journal (Aug. 2, 2019), available at: <https://www.hipaajournal.com/first-half-of-2019-sees-31-million-healthcare-records-breached>.

incidents.<sup>12</sup> Conditions have only worsened since: Statista estimates that “[i]n 2019, the number of data breaches in the United States amounted to 1,473 with over 164.68 million sensitive records exposed[,]” and that “[i]n the first half of 2020, there were 540 reported data breaches.”<sup>13</sup>

58. Securing PII is particularly important in light of the high-profile data breaches that have been reported in recent years, of which a sophisticated entity like Navistar knew or should have known,<sup>14</sup> including data breaches at: Arby’s, Chipotle, Dairy Queen, Forever 21, GameStop, Harbor Freight Tools, Home Depot, Hy-Vee, Kmart, Lord & Taylor, Michael’s Stores, Neiman Marcus, Noodles & Co., P.F. Chang’s, Saks Fifth Avenue, Sally Beauty Supply, Schnuck Markets, Sonic Drive-In, SuperValu, Target, T.J. Maxx, Wendy’s, Sony, General Electric and many others.

59. As major companies like Sony, General Electric, and even the United States government itself have learned, employee records like those misappropriated during the Data Breach make a particularly enticing target. Unlike the records held by retailers and misappropriated through payment system hacks—which consist largely of payment card information that affected individuals can change and thereby protect—employee records offer a treasure trove of immutable PII, such as dates of birth and Social Security Numbers, which criminals can use to steal and abuse an individual’s identity for years to come.

---

<sup>12</sup> *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2020*, Statista, <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-unitedstates-by-number-of-breaches-and-records-exposed> (last visited Oct. 20, 2021).

<sup>13</sup> *Id.*

<sup>14</sup> Indeed, Navistar acknowledges in its filings to the SEC that it has previously experienced cyber-attacks and attempts to breach its systems. *See* Form 10-K, U.S. Securities and Exchange Commission, available at: <https://www.sec.gov/ix?doc=/Archives/edgar/data/808450/000080845020000105/nav10k2020.htm>.

60. Data breaches are a constant threat, however, because of the price that PII fetches on the dark web. That is particularly true of PHI, which according to Experian sells on the dark web for prices hundreds or thousands of times that of basic personal or financial information.<sup>15</sup>

61. When a data breach occurs—especially when the breach concerns medical or financial information—victims must spend significant time, energy, and effort to protect themselves. Cybercriminals use PII to commit identity theft in order to commit fraudulent transactions and obtain consumer credit using the victim’s information.

62. Data breaches involving medical and health information, like the one here at issue, amplify those risks considerably because of the access it provides to criminals.

63. When the PII includes medical information, the identity theft could extend to sending the victim fake medical bills or obtaining medical services using the victim’s insurance and PHI or PII, which can result in unknown, unpaid bills being sent to collections, causing further harm to data breach victims.<sup>16</sup>

64. Moreover, unlike victims of breaches involving only financial information, victims of data breaches involving sensitive and immutable PII and PHI cannot simply “reverse” fraudulent transactions.<sup>17</sup> For example, one study found that the majority of medical identity theft victims had to pay an average of \$13,500 to resolve issues stemming from the data breach, and

---

<sup>15</sup> See Brian Stack, *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>.

<sup>16</sup> Medical Identity Theft, Federal Trade Commission (Jan. 2011), available at: <https://www.bulkorder.ftc.gov/system/files/publications/bus75-medical-identity-theft-faq-health-care-health-plan.pdf>.

<sup>17</sup> See *The \$300 Billion Attack: The Revenue Risk and Human Impact of Healthcare Provider Cyber Security Inaction*, Accenture (2015).



only 10% of victims achieved a completely satisfactory resolution.<sup>18</sup> Almost one-third of medical identity theft victims also lost their health insurance as a result of the identity theft.<sup>19</sup>

65. As Kunal Rupani, director of product management at Accellion, a private cloud solutions company, explained in the context of a different medical data breach:

Unlike credit card numbers and other financial data, healthcare information doesn't have an expiration date. As a result, a patient's records can sell on the black market for upwards of fifty times the amount of their credit card number, making hospitals and other healthcare organizations extremely lucrative targets for cybercriminals.<sup>20</sup>

66. SecureWorks, a division of Dell Inc., echoed that sentiment, noting that “[i]t’s a well known truism within much of the healthcare data security community that an individual healthcare record is worth more on the black market (\$50, on average) than a U.S.-based credit card and personal identity with social security number combined.”<sup>21</sup> The reason is that thieves “[c]an use a healthcare record to submit false medical claims (and thus obtain free medical care), purchase prescription medication, or resell the record on the black market.”<sup>22</sup>

67. Similarly, the FBI Cyber Division in an April 8, 2014 Private Industry Notification, advised:

Cyber criminals are selling [medical] information on the black market at a rate of \$50 for each partial EHR, compared to \$1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.<sup>23</sup>

---

<sup>18</sup> See *Fifth Annual Study on Medical Identity Theft*, Ponemon Institute LLC (Feb. 2015), at pp.2, 7, available at: [https://static.nationwide.com/static/2014\\_Medical\\_ID\\_Theft\\_Study.pdf?r=65](https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65).

<sup>19</sup> *Id.*

<sup>20</sup> Jeff Goldman, 21st Century Oncology Notifies 2.2 Million Patients of Data Breach (Mar. 11, 2016), <http://www.esecurityplanet.com/network-security/21st-century-oncology-notifies-2.2-million-patients-of-data-breach.html>.

<sup>21</sup> What’s the Market Value of a Healthcare Record, Dell SecureWorks (Dec. 13, 2012), <https://www.secureworks.com/blog/general-market-value-of-a-healthcare-record>.

<sup>22</sup> *Id.*

<sup>23</sup> *FBI Cyber Division Private Industry Notification*, Federal Bureau of Investigation (Apr. 8, 2014), <https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf>.

68. In addition, the Federal Trade Commission (“FTC”) has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of personal data, including recent cases concerning health-related information against LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Defendant on notice of their obligation to safeguard PII.

69. The risks identity theft poses can persist indefinitely, and for now and years to come Plaintiff and Class members will suffer the significant and concrete risk that their PII will be (or already has been) misappropriated, and that their identities will be stolen.

70. Other categories of PII compromised in the Data Breach pose lifelong concerns. While individuals can change credit card numbers or open a new bank account in response to a breach, Plaintiff and the Class cannot change their Social Security or driver’s license numbers.

71. Neal O’Farrell, a security and identity theft expert for Credit Sesame, calls a Social Security number “your secret sauce,” that is “as good as your DNA to hackers.”<sup>24</sup>

72. Unfortunately, Plaintiff and Class members will have to wait until they become victims of Social Security number misuse before they can obtain a new one. But even then, the Social Security Administration warns “that a new number probably won’t solve all [] problems . . . and won’t guarantee . . . a fresh start.” In fact, “[f]or some victims of identity theft, a new number actually creates new problems.”<sup>25</sup> One of those new problems is that a new Social Security number will have a completely blank credit history, making it difficult to get credit for years unless it is linked to the old compromised number.

---

<sup>24</sup> Cameron Huddleston, *How to Protect Your Kids from the Anthem Data Breach*, Kiplinger (Feb. 11, 2015), [www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html](http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html).

<sup>25</sup> *Identity Theft and Your Social Security Number*, Social Security Admin. (July 2021), at pp. 6-7, <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

***Navistar had a Duty and Obligation to Protect PII and PHI***

73. Defendant has an obligation, both statutory and self-imposed, to keep confidential and protect from unauthorized access and/or disclosure Plaintiff's and the Class' PII. Defendant's obligations are derived from: 1) government regulations, including the Illinois Personal Information Protection Act ("PIPA"), 815 ILCS 530/1, *et seq.*, and similar state laws, HIPAA, and FTC rules and regulations; 2) industry standards; and 3) promises and representations regarding the handling of sensitive PII. Plaintiff and Class members provided, and Defendant obtained, their PII on the understanding that Defendant would protect and keep the PII from unauthorized access or disclosure.

74. HIPAA requires, *inter alia*, that Covered Entities and Business Associates like Defendant implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of PII, protect against any reasonably anticipated threats or hazards to the security or integrity of PII, regularly review access to databases containing protected information, implement and maintain procedures and systems intended to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

75. Additionally, HIPAA requires Covered Entities and Business Associates to provide notification to every affected individual following the impermissible use or disclosure of any protected health information. The individual notice must be provided to affected individuals without unreasonable delay and no later than 60 days following discovery of the breach. Further, for a breach involving more than 500 individuals, entities are required to provide notice in prominent media outlets. *See* 45 CFR § 164.400, *et seq.*

76. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.<sup>26</sup>

77. Further, the FTC's Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, and notify the media and the FTC as well. *See* 16 CFR 318.1, *et seq.*

78. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.<sup>27</sup> The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.<sup>28</sup> The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.<sup>29</sup> Defendant clearly failed to do any of the foregoing, as evidenced by the length of, and the amount of data exfiltrated during, the Data Breach.

79. Here, at all relevant times, Defendant was fully aware of its obligation to protect the PII and PHI of current and former employees and their family members, including Plaintiffs

---

<sup>26</sup> *Start With Security*, Federal Trade Commission (June 2015), available at

<https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

<sup>27</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Jan. 23, 2015), available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

<sup>28</sup> *Id.*

<sup>29</sup> *Id.*

and the Class, because it is a sophisticated and technologically savvy business entity that relies extensively on information technology systems and networks, and routinely maintains and transmits PII in order to operate its business.

80. Defendant, as the current and/or former employer of Plaintiff and the Class, had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the PII and PHI of current and former employees and their family members from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendant and its employees, and Defendant's requirement that employees and their family members submit their sensitive, non-public personal information, such as their PII and PHI, to Defendant for purposes of employment and/or participation in the Navistar Health Plan and Navistar Retiree Health Benefit and Life Insurance Plan. Defendant alone had the exclusive ability to implement adequate security measures on its computer systems to secure and protect Plaintiff's and Class members' PII and PHI.

81. Defendant also was aware of the significant consequences of its failure to do so because it collected sensitive information, including PII and PHI, from thousands of employees annually, and knew that this data, if hacked, would injure current and former employees, including Plaintiffs and Class members.

82. Defendant's failure to follow the FTC guidelines and its subsequent failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data constitute unfair acts or practices prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 14 U.S.C. § 45.

83. Additionally, Defendant had a duty to notify Plaintiff and Class members that their PII and/or PHI was accessed by unauthorized persons, especially when Defendant knew that the highly sensitive and personal information was being sold on the internet.

***Defendant Violated HIPAA, FTC, and Industry Standard Data Protection Protocols***

84. HIPAA obligates Covered Entities and Business Associates to adopt administrative, physical, and technological safeguards to ensure the confidentiality, integrity, and security of PII and PHI.

85. The FTC rules, regulations, and guidelines obligate business to protect PII and PHI, from unauthorized access or disclosure by unauthorized persons.

86. Unfortunately, Defendant failed to comply with PIPA, HIPAA, FTC rules, regulations and guidelines, and industry standards concerning the protection and security of PII. As evidenced by the duration, scope and nature of the Data Breach, among its many deficient practices, Defendant failed in, *inter alia*, the following respects:

- a. Developing and employing adequate intrusion detection systems;
- b. Creating effective employee training on phishing attempts;
- c. Engaging in regular reviews of audit logs and authentication records;
- d. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;
- e. Ensuring the confidentiality and integrity of current and former employees' PII and PHI;
- f. Protecting against any reasonably anticipated threats or hazards to the security or integrity of current and former employees' PII and PHI;

- g. Implementing policies and procedures to prevent, detect, contain, and correct security violations;
- h. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;
- i. Implementing technical policies, procedures and safeguards for electronically stored information concerning protected health and medical information that permit access for only those persons or programs that have specifically been granted access; and
- j. Other similar measures to protect the security and confidentiality of current and former employees' PII and PHI.

87. Had Defendant implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. Defendant could have prevented or detected the Data Breach prior to the hackers accessing Defendant's systems and extracting sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and current and former employees would have been notified sooner, allowing them to promptly take protective and mitigating actions.

***Defendant's Data Security Practices are Woefully Inadequate and Inconsistent with its Self-Imposed Data Security Obligations***

88. Defendant purports to care about data security and safeguarding employees' PII, and represents that it will keep secure and confidential the PII that current and former employees

provided. Specifically, Defendant represents that it keeps sensitive PII using a “robust program of information security and controls.”<sup>30</sup>

89. Plaintiff and the Class thus entrusted their PII to Defendant in reliance on its promises and self-imposed obligations to keep their PII confidential, and to secure their PII from unauthorized access by malevolent actors. It failed to do so in violation of its own privacy policies.

90. The length of the Data Breach also demonstrates that Defendant failed to safeguard PII by, *inter alia*: maintaining an adequate data security environment to reduce the risk of a data breach; periodically auditing its security systems to discover intrusions like the Data Breach; and retaining outside vendors to periodically test its network, servers, systems and workstations.

91. Had Defendant undertaken the actions that federal and state law required it to take, the Data Breach could have been prevented or the consequences of the Data Breach significantly reduced, as Defendant would have detected the Data Breach prior to the hackers extracting data from Defendant’s systems, and current and former employees would have been notified of the Data Breach sooner, allowing them to take necessary protective or mitigating measures much earlier.

92. Indeed, following the Data Breach, Defendant effectively conceded that its security practices prior thereto were inadequate and ineffective. In the First and Second Notice letters it belatedly sent to Plaintiff and others, Defendant acknowledged that the Data Breach required it to implement multiple remedial measures “to enhance [its] security protocols and controls, technology, and training[.]”<sup>31</sup> remedial measures that, on information and belief, consist of the

---

<sup>30</sup> Form 10-K, U.S. Securities and Exchange Commission (Oct. 31, 2020), available at: <https://www.sec.gov/ix?doc=/Archives/edgar/data/808450/000080845020000105/nav10k2020.htm>.

<sup>31</sup> First Notice, Exhibit A; Second Notice, Exhibit B.



above-referenced policies and procedures, which Navistar would already have had in place had it complied with its legal obligations and followed industry best-practices.

***Plaintiff and Class Members Suffered Harm Resulting from the Data Breach***

93. Like any data hack, the Data Breach presents major problems for all affected. According to Jonathan Bowers, a fraud and data specialist at fraud prevention provider Trustev, “Give a fraudster your comprehensive personal information, they can steal your identity and take out lines of credit that destroy your finances for years to come.”<sup>32</sup>

94. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, “[t]hat’s what thieves use most often to commit fraud or identity theft.” And once they have this information, “they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance.”<sup>33</sup>

95. The ramifications of Defendant’s failure to properly secure PII, including Plaintiff’s and Class members’ PII, are severe. Identity theft occurs when someone uses another person’s medical, financial, and personal information, such as that person’s name, address, Social Security number, medical and insurance information, and other information, without permission to commit fraud or other crimes.

96. According to data security experts, one out of every four data breach notification recipients becomes a victim of identity fraud.

97. In response to the Data Breach, Defendant offered to provide certain individuals whose PII and/or PHI was exposed in the Data Breach with two years of credit monitoring. Victims

---

<sup>32</sup> Roger Cheng, *Data Breach Hits Roughly 15M T-Mobile Customers, Applicants*, CNET (Oct. 1, 2015), available at: <http://www.cnet.com/news/data-breach-snags-data-from-15m-t-mobile-customers/>.

<sup>33</sup> *What to Know About Identity Theft*, Federal Trade Comm’n (March 2021), available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft>.

of the Data Breach who were offered the credit monitoring had a small window—only a couple of months from the issuance of the First Notice—to receive the written notice and sign up for the credit monitoring.<sup>34</sup>

98. Moreover, the credit monitoring offered by Defendant to certain victims of the Data Breach is inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive PII and/or PHI.

99. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

- a. Theft of PII, including medical information;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the PII and/or PHI stolen during the Data Breach;
- c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;
- d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, notifying their health insurance providers that their protected medical and health information was accessed by unauthorized persons, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, *if* they were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice in accordance with state law;
- e. The imminent and impending injury resulting from potential fraud and identity theft posed because their PII and/or PHI is exposed for theft and sale on the dark web; and

---

<sup>34</sup> When Defendant disclosed the exposure and exfiltration of additional PII and PHI in the Second Notice, it extended the deadline to sign up for credit monitoring to approximately three months after the date of the Second Notice.

f. The loss of Plaintiff's and Class members' privacy.

100. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII and/or PHI being accessed by cybercriminals, risks that will not abate within a mere two years: the unauthorized access of Plaintiff's and Class members' PII and PHI, especially their Social Security numbers and medical information, puts Plaintiff and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Defendant offered victims of the Breach. The two years of credit monitoring that Defendant offered to certain victims of the Data Breach is inadequate to mitigate the aforementioned injuries Plaintiff and Class suffered as a result of the Data Breach.

101. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure current and former employees' PII, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

102. Plaintiff retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both himself and similarly situated individuals whose PII and/or PHI was accessed in the Data Breach.

103. Defendant is aware of the ongoing harm that the Data Breach has and will continue to impose on current and former employees, as the notices that it posted and sent to regarding the Data Breach advise the victims to review their account statements and credit reports for fraudulent or questionable activity.

### **CLASS ALLEGATIONS**

104. Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

All persons in the United States whose PII and/or PHI was accessed in the Data Breach, that was disclosed to the United States Securities and Exchange Commission on June 7, 2021.

Excluded from the Class are Defendant, its executives, officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

105. In the alternative, Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

All persons in Illinois whose PII and/or PHI was accessed in the Data Breach, that was disclosed to the United States Securities and Exchange Commission on June 7, 2021 (the “Illinois Subclass”).

Excluded from the Illinois Subclass are Defendant, its executives, officers, and the Judge(s) assigned to this case.

106. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiff only through the discovery process, Plaintiff believes, and on that basis alleges, that thousands of individuals comprise the Class and were affected by the Data Breach, because Defendant is one of the largest vehicle manufacturers and commercial vehicle service parts distributors in the United States, with a network of more than 1,000 dealers and numerous service partners throughout North America. The members of the Class will be identifiable through information and records in Defendant’s possession, custody, and control.

107. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

- a. Whether Defendant's data security and retention policies were unreasonable;
- b. Whether Defendant failed to protect the confidential and highly sensitive information with which it was entrusted;
- c. Whether Defendant owed a duty to Plaintiff and Class members to safeguard their PII and/or PHI;
- d. Whether Defendant breached any legal duties in connection with the Data Breach;
- e. Whether Defendant's conduct was intentional, reckless, willful or negligent;
- f. Whether an implied contract was created concerning the security of Plaintiff's and Class members' PII and/or PHI;
- g. Whether Defendant breached that implied contract by failing to protect and keep secure Plaintiff's and Class members' PII and/or PHI and/or failing to timely and adequately notify Plaintiff and Class members of the Data Breach;
- h. Whether Plaintiff and Class members suffered damages as a result of Defendant's conduct; and
- i. Whether Plaintiff and Class Members are entitled to monetary damages, injunctive relief and/or other remedies and, if so, the nature of any such relief.

108. Typicality: All of Plaintiff's claims are typical of the claims of the Class since Plaintiff and all members of the Class had their PII and/or PHI compromised in the Data Breach. Plaintiff and the members of the Class sustained damages as a result of Defendant's uniform wrongful conduct.

109. Adequacy: Plaintiff is an adequate representative because his interests do not materially or irreconcilably conflict with the interests of the Class he seeks to represent, he has retained counsel competent and highly experienced in complex class action litigation, and intends to prosecute this action vigorously. Plaintiff and his counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor his counsel have any interests that are antagonistic to the interests of other members of the Class.

110. Superiority: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and members of the Class. The injury suffered by

each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. 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. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases.

111. Defendant has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final relief with respect to the Class as a whole.

**CAUSES OF ACTION AND CLAIMS FOR RELIEF**

**COUNT I — Negligence**

**(On behalf of Plaintiff, the Class, and the Illinois Subclass)**

112. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

113. This count is brought on behalf of all Class members.

114. Defendant owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the PII and PHI that Defendant collected.

115. Defendant owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PII and PHI that Defendant collected.

116. Defendant owed a duty to Plaintiff and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it is discovered.

117. Defendant owed a duty of care to Plaintiff and the Class because they were a foreseeable and probable victim of any inadequate data security practices.

118. Defendant solicited, gathered, and stored the PII and PHI provided by Plaintiff and the Class.

119. Defendant knew or should have known it inadequately safeguarded this information.

120. Defendant knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiff and the Class, and Defendant was therefore charged with a duty to adequately protect this critically sensitive information.

121. Defendant had a special relationship with Plaintiff and the Class. Plaintiff's and the Class' willingness to entrust Defendant with their PII and PHI was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PII and PHI stored on them from attack.

122. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and the Class and their PII and PHI. Defendant's misconduct included failing to: (1) secure its systems, servers and workstations, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the safeguards, policies, and procedures necessary to prevent this type of data breach.

123. Defendant breached its duties to Plaintiff and the Class by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiff and Class members.

124. Defendant breached its duties to Plaintiff and Class members by creating a foreseeable risk of harm through the misconduct previously described.

125. Defendant breached the duties it owed to Plaintiff and the Class by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of PII and PHI.

126. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII and PHI to Plaintiff and the Class so that Plaintiff and the Class could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII and PHI.

127. Defendant breached the duties it owed to Plaintiff and the Class by failing to timely and accurately disclose to Plaintiff and the Class members that their PII and PHI had been improperly acquired or accessed.

128. Defendant breached its duty to timely notify Plaintiff and the Class of the Data Breach by failing to provide direct notice to Plaintiff and Class members concerning the Data Breach until (at earliest) July 6, 2021, and failing to provide direct notice to Plaintiff and Class members that additional PII, including their PHI, had been accessed and exfiltrated until September 21, 2021.

129. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered a drastically increased risk of identity theft, relative to both the time period



before the breach, as well as to the risk born by the general public, as well as other damages, including but not limited to time and expenses incurred in mitigating the effects of the Data Breach.

130. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT II – Negligence *Per Se***  
**(On behalf of Plaintiff, the Class, and the Illinois Subclass)**

131. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

132. This count is brought on behalf of all Class members.

133. HIPAA obligates Covered Entities and Business Associates to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information” and “must reasonably safeguard protected health information.” 45 CFR § 164.530(c).

134. In the event of a data breach, HIPAA obligates Covered Entities and Business Associates to notify affected individuals, prominent media outlets, and the Secretary of the Department of Health and Human Services of the data breach without unreasonable delay and in no event later than 60 days after discovery of the data breach. 45 CFR § 164.400, *et seq.*

135. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to protect PII and/or PHI. Various FTC publications and orders also form the basis of Defendant's duty.

136. The Illinois Personal Information Protection Act (“PIPA”), 815 ILCS 530/1, *et seq.*, obligates “data collectors” that own, license, maintain or store records that contain personal information of Illinois residents to “implement and maintain reasonable security measures to

protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. 815 ILCS 530/45.

137. Additionally, the PIPA creates a duty for data collectors to notify Illinois residents of any data breach “immediately following discovery” of the data breach. 815 ILCS 530/10(b).

138. Defendant violated PIPA, HIPAA and FTC rules and regulations obligating companies to use reasonable measures to protect PII and PHI by failing to comply with applicable industry standards; and by unduly delaying reasonable notice of the actual breach. Defendant’s conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored, the foreseeable consequences of a Data Breach and the exposure of Plaintiff’s and Class members’ sensitive PII and PHI.

139. Defendant’s violations of PIPA, HIPAA and Section 5 of the FTC Act constitutes negligence *per se*.

140. Plaintiff and the Class are within the category of persons PIPA, HIPAA and the FTC Act were intended to protect.

141. The harm that occurred as a result of the Data Breach described herein is the type of harm PIPA, HIPAA and the FTC Act were intended to guard against.

142. As a direct and proximate result of Defendant’s negligence *per se*, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII and PHI in Defendant’s possession, and are entitled to damages in an amount to be proven at trial.

**COUNT III – Breach of Implied Contract**  
**(On behalf of Plaintiff, the Class, and the Illinois Subclass)**

143. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

144. This count is brought on behalf of all Class members.

145. As a condition of their employment by Navistar, Plaintiff and Class members provided Defendant with their PII. Additionally, as a condition of their participation in the Navistar Health Plan and/or Navistar Retiree Health Benefit and Life Insurance Plan, Plaintiff and Class members provided Defendant with their PII and PHI.

146. By providing their PII and PHI, and upon Defendant's acceptance of such information, Plaintiff and Class members, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

147. The implied contracts between Defendant and Class members obligated Defendant to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' PII and PHI. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. Defendant expressly adopted and assented to these terms in its public statements, representations and promises as described above.

148. The implied contracts for data security also obligated Defendant to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their PII or PHI.

149. Defendant breached the implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the PII and PHI of Plaintiff and Class members and allowing unauthorized persons to access Plaintiff's and Class members' PII and PHI, and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

150. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and the Class have been damaged as described herein, will continue to suffer injuries as

detailed above due to the continued risk of exposure of their PII and PHI in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

**COUNT IV – Bailment**  
**(On behalf of Plaintiff, the Class, and the Illinois Subclass)**

151. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

152. This count is brought on behalf of all Class members.

153. As a requirement of their employment by Defendant, and their participation in the Navistar Health Plan and/or Navistar Retiree Health Benefit and Life Insurance Plan, Plaintiff and Class members were provided their PII and/or PHI to Defendant.

154. In delivering their personal information to Defendant, Plaintiff and Class members intended and understood that Defendant would adequately safeguard their PII and PHI.

155. Defendant accepted Plaintiff's and Class members' PII and PHI.

156. By accepting possession of Plaintiff's and Class members' PII and PHI, Defendant understood that Plaintiff and Class members expected Defendant to adequately safeguard their PII and PHI. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

157. During the bailment (or deposit), Defendant owed a duty to Plaintiff and Class members to exercise reasonable care, diligence and prudence in protecting their PII and PHI.

158. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' PII and PHI, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class members' PII and PHI.

159. Defendant further breached its duty to safeguard Plaintiff's and Class members' PII and PHI by failing to timely notify them that their PII and/or PHI had been compromised as a result of the Data Breach.

160. Defendant failed to return, purge or delete the PII and/or PHI of Plaintiff and members of the Class at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

161. As a direct and proximate result of Defendant's breach of its duties, Plaintiff and Class members suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth herein.

162. As a direct and proximate result of Defendant's breach of its duty, the PII and PHI of Plaintiff and Class members entrusted to Defendant during the bailment (or deposit) was damaged and its value diminished.

**COUNT V – Violation of the Illinois Personal Information Protection Act**  
**(On behalf of Plaintiff and the Illinois Subclass)**

163. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

164. This count is brought on behalf of all Illinois Subclass members.

165. The Illinois Personal Information Protection Act (“PIPA”), 815 ILCS 530/1, *et seq.*, obligates “data collectors” that own, license, maintain or store records that contain personal information of Illinois residents to “implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.” 815 ILCS 530/45.

166. Additionally, the PIPA creates a duty for data collectors to notify Illinois residents of any data breach “immediately following discovery” of the data breach. 815 ILCS 530/10(b).

167. Defendant is a “data collector” as defined by PIPA.

168. Defendant failed to implement and maintain reasonable security measures to safeguard, protect and keep confidential Plaintiff's and Illinois Subclass members' PII from unauthorized access or disclosure, as alleged herein.

169. Defendant, knowing and/or reasonably believing that Plaintiff's and Illinois Subclass members' PII was acquired or accessed by unauthorized persons during the Data Breach, failed to provide prompt, immediate, and reasonable notice of the Data Breach to Plaintiff and the Illinois Subclass as required by PIPA.

170. Defendant's failure to implement and maintain reasonable security measures to protect current and former employees' PII, and/or Defendant's failure to provide timely and accurate notice of the Data Breach violated the PIPA.

171. As a result of Defendant's failure to reasonably safeguard the PII belonging to Plaintiff and the Illinois Subclass, and Defendant's failure to provide reasonable and timely notice of the Data Breach to Plaintiff and the Illinois Subclass, Plaintiff and the Illinois Subclass have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

**COUNT VI – Violation of the Illinois Consumer Fraud and Deceptive Practices Act**  
**(On behalf of Plaintiff and the Illinois Subclass)**

172. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

173. This count is brought on behalf of all Illinois Subclass members.

174. The Illinois Consumer Fraud and Deceptive Business Practices Act ("IFCA") prohibits "unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact. . . ." 815 ILCS 505/2.

175. Plaintiff and the Illinois Subclass are entitled to sue under ICFA as Defendant's conduct implicates significant consumer protections concerns. Navistar failed to disclose that it did not implement adequate security measures to protect and safeguard PII and PHI with the intent that Plaintiff and Class members would enter into an employment relationship with Navistar and/or participate in the Navistar Health Plan or Navistar Retiree Health Benefit and Life Insurance Plan. Plaintiff and members of the Illinois Subclass, acting as consumers, participated in the Navistar Health Plan or Navistar Retiree Health Benefit and Life Insurance Plan, and thereby provided their PII and PHI to Navistar.

176. Defendant is a "person" as those terms are defined by the ICFA.

177. Plaintiff and members of the Illinois Subclass participated in the Navistar Health Plan and/or Navistar Retiree Health Benefit and Life Insurance Plan primarily for personal, family or household purposes.

178. Defendant's actions, as set forth above, occurred in the course of trade or commerce.

179. Defendant's unlawful, unfair, deceptive, fraudulent and/or unconscionable acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass members' PII and/or PHI, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass members' PII and/or PHI, including but not limited to duties imposed by PIPA, HIPAA and the FTC Act, which were direct and proximate causes of the Data Breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Illinois Subclass members' PII and/or PHI, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and the Illinois Subclass members' PII and/or PHI;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Illinois Subclass members' PII and/or PHI;
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass members' PII and/or PHI; and
- h. Failing to promptly and adequately notify Plaintiff and Illinois Subclass members that their PII and/or PHI was accessed by unauthorized persons in the Data Breach.

180. Defendant's conduct constitutes unconscionable, deceptive, and unfair acts and practices.

181. Defendant's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and its ability to protect the confidentiality of current and former employees' PII and/or PHI.

182. Defendant intentionally, knowingly, and maliciously mislead Plaintiff and Illinois Subclass members and induced them to rely on its misrepresentations and omissions.

183. Had Defendant disclosed to Plaintiff and Illinois Subclass members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Illinois Subclass members' PII and/or PHI without advising them that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their PII and/or PHI. Accordingly, Plaintiff and the Illinois Subclass members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.



184. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws like PIPA, HIPAA and the FTC Act.

185. The injuries suffered by Plaintiff and Illinois Subclass members greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiff and Illinois Subclass members should have reasonably avoided.

186. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and Class members as a direct result of Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices as set forth in this Complaint include, without limitation:

- a. unauthorized charges on their debit and credit card accounts;
- b. theft of their PII and/or PHI;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;
- e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, informing their health insurance providers that their PII and/or PHI was exposed in the Data Breach, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

- f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;
- g. damages to and diminution in value of their personal information entrusted to Defendant for the purpose of employment and/or participating in the Navistar Health Plan and/or Navistar Retiree Health Benefit and Life Insurance Plan, and with the understanding that Defendant would safeguard their data against theft and not allow access and misuse of their data by others; and
- h. the continued risk to their PII and/or PHI, 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 data in its possession.

187. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PII or PHI without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

**COUNT VII – Violation of the Illinois Consumer Fraud and Deceptive Practices Act**  
**Vis-à-Vis Violations of the Illinois Personal Information Protection Act**  
**(On behalf of Plaintiff and the Illinois Subclass)**

188. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

189. This count is brought on behalf of all Illinois Subclass members.

190. A violation of the PIPA constitutes an unlawful practices in violation of ICFA. 815 ILCS 530/20.

191. As described above, Defendant failed to implement and maintain reasonable security measures to safeguard, protect and keep confidential Plaintiff's and Illinois Subclass members' PII from unauthorized access or disclosure, as alleged herein.

192. Defendant, knowing and/or reasonably believing that Plaintiff's and Illinois Subclass members' PII was acquired or accessed by unauthorized persons during the Data Breach,

failed to provide prompt, immediate, and reasonable notice of the Data Breach to Plaintiff and the Illinois Subclass as required by PIPA.

193. Defendant's failure to implement and maintain reasonable security measures to protect current and former employees' PII, and/or Defendant's failure to provide timely and accurate notice of the Data Breach violated the PIPA.

194. By violating PIPA, Defendant's conduct constitutes an unlawful practice in violation of the ICFA.

195. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

**COUNT VIII – Violation of State Consumer Protection Statutes**  
**(On behalf of Plaintiff, the Class, and the Subclass)**

196. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

197. This count is brought on behalf of all Class members.

198. Defendant is a "person" as defined in the relevant state consumer statutes.

199. Defendant engaged in the conduct alleged herein in transactions intended to result, and which did result, in the sale of goods or services to consumers. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Further, Defendant's conduct implicates consumer protection concerns generally.

200. Defendant's acts, practices and omissions were done in the course of Defendant's business of marketing, facilitating, offering for sale, and selling goods and services throughout the United States.

201. Defendant's unlawful, unfair, deceptive, fraudulent and/or unconscionable acts and practices include:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII and/or PHI, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which was a direct and proximate cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII and/or PHI, including but not limited to duties imposed by HIPAA and the FTC Act, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII and/or PHI, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and the Class members' PII and/or PHI;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII and/or PHI;
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII and/or PHI; and
- h. Failing to promptly and adequately notify Plaintiff and Class members that their PII and/or PHI was accessed by unauthorized persons in the Data Breach.

202. By engaging in such conduct and omissions of material facts, Defendant has violated state consumer laws prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," representing that "goods and services are of a particular standard, quality or grade, if they are of another", and/or "engaging in any other conduct which similarly creates a likelihood of confusion

or of misunderstanding”); and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

203. Defendant’s representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of Defendant’s data security and ability to protect the confidentiality of PII.

204. Defendant intentionally, knowingly, and maliciously misled Plaintiff and Class members and induced them to rely on its misrepresentations and omissions.

205. Had Defendant disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiff’s and Class members’ PII without advising them that Defendant data security practices were insufficient to maintain the safety and confidentiality of their PII and/or PHI. Accordingly, Plaintiff and the Class members acted reasonably in relying on Defendant’s misrepresentations and omissions, the truth of which they could not have discovered.

206. Past breaches within the industry and against Defendant itself put Defendant on notice that its security and privacy protections were inadequate.

207. Defendant’s practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws like HIPAA and the FTC Act.

208. The harm these practices caused to Plaintiff and the Class members outweighed their utility, if any.

209. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and Class members as a direct result of Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices as set forth herein include, without limitation:

- a. unauthorized charges on their debit and credit card accounts;
- b. theft of their PII and/or PHI;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;
- e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, informing their health insurance providers that their PII and/or PHI was exposed in the Data Breach, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;
- f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;
- g. damages to and diminution in value of their personal and financial information entrusted to Defendant for the purpose of employment and/or participating in the Navistar Health Plan and/or Navistar Retiree Health Benefit and Life Insurance Plan, and with the understanding that Defendant would safeguard their data against theft and not allow access and misuse of their data by others;
- h. the continued risk to their PII and/or PHI, 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 data in its possession.

210. Defendant's conduct described herein, including without limitation, Defendant's failure to maintain adequate computer systems and data security practices to safeguard current and former employees' PII and PHI, Defendant's failure to disclose the material fact that it did not have adequate computer systems and safeguards to adequately protect current and former employees' PII and PHI, Defendant's failure to provide timely and accurate notice to of the material fact of the Data Breach, and Defendant's continued acceptance of Plaintiff's and Class members' PII and/or PHI constitute unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices in violation of the following state consumer statutes:

- a. The Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5(5), (7) and (27), *et seq.*;
- b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;
- c. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq.*, and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq.*;
- d. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq.*;
- e. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-393(a) and (b)(2), (5) and (7), *et seq.*;
- f. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), *et seq.*; and Idaho Code § 48-603C, *et seq.*;
- g. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq.*, and the Illinois Uniform Deceptive Trades Practices Act, 815 Ill. Stat. § 510/2(a)(5), (7) and (12), *et seq.*;
- h. The Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), and (iv) and (9)(i), *et seq.*;
- i. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), *et seq.*;
- j. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq.*;

- k. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915(5) and (7), *et seq.*;
- l. New York Business Law, N.Y. Gen. Bus. Law § 349(a);
- m. The North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), *et seq.*;
- n. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq.*;
- o. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-4(1) and (2)(a) and (b);
- p. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(5)(6) and (14), *et seq.*; and
- q. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq.*

211. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PII and/or PHI without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

**COUNT IX – Violation of State Data Breach Statutes**  
**(On behalf of Plaintiff, the Class, and the Illinois Subclass)**

212. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

213. This count is brought on behalf of all Class members.

185. Defendant is a business that owns, maintains, and licenses PII, and computerized data including PII, about Plaintiff and Class members.

191. Defendant is in possession of PII belonging to Plaintiff and the Class and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.



192. Defendant failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by all applicable State laws.

193. Defendant, knowing and/or reasonably believing that Plaintiff's and Class members' PII was acquired by unauthorized persons during the Data Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiff and the Class as required by following data breach statutes.

194. Defendant's failure to provide timely and accurate notice of the data breach violated the following state data breach statutes:

- a. Alaska Stat. Ann. § 45.48.010(a), *et seq.*;
- b. Ark. Code Ann. § 4-110-105(a), *et seq.*;
- c. Cal. Civ. Code § 1798.83(a), *et seq.*;
- d. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;
- e. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq.*;
- f. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq.*;
- g. D.C. Code § 28-3852(a), *et seq.*;
- h. Fla. Stat. Ann. § 501.171(4), *et seq.*;
- i. Ga. Code Ann. § 10-1-912(a), *et seq.*;
- j. Haw. Rev. Stat. § 487N-2(a), *et seq.*;
- k. Idaho Code Ann. § 28-51-105(1), *et seq.*;
- l. Ill. Comp. Stat. Ann. 530/10(a), *et seq.*;
- m. Iowa Code Ann. § 715C.2(1), *et seq.*;
- n. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;
- o. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;

- p. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;
- q. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;
- r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), *et seq.*;
- s. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;
- t. Minn. Stat. Ann. § 325E.61(1)(a), *et seq.*;
- u. Mont. Code Ann. § 30-14-1704(1), *et seq.*;
- v. Neb. Rev. Stat. Ann. § 87-803(1), *et seq.*;
- w. Nev. Rev. Stat. Ann. § 603A.220(1), *et seq.*;
- x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;
- y. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;
- z. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;
- aa. N.D. Cent. Code Ann. § 51-30-02, *et seq.*;
- bb. Okla. Stat. Ann. Tit. 24 § 163(A), *et seq.*;
- cc. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;
- dd. R.I. Gen. Laws Ann. § 11-49.3-4(a)(1), *et seq.*;
- ee. S.C. Code Ann. § 39-1-90(A), *et seq.*;
- ff. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;
- gg. Tex. Bus. & Com. Code Ann. § 521.053(b), *et seq.*;
- hh. Utah Code Ann. § 13-44-202(1), *et seq.*;
- ii. Va. Code. Ann. § 18.2-186.6(B), *et seq.*;
- jj. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*;
- kk. Wis. Stat. Ann. § 134.98(2), *et seq.*; and
- ll. Wyo. Stat. Ann. § 40-12-502(a), *et seq.*

214. As a result of Defendant's failure to reasonably safeguard the Plaintiff's and Class members' PII, and Defendant's failure to provide reasonable and timely notice of the Data Breach

to its current and former employees, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

**COUNT X – Declaratory Judgment**  
**(On behalf of Plaintiff, the Class, and the Illinois Subclass)**

215. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

216. This count is brought on behalf of all Class members.

217. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described herein.

218. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard its current and former employees' PII and PHI, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their PII and/or PHI. Plaintiff alleges that Defendant's data security measures remain inadequate.

219. Plaintiff and Class members continue to suffer injury as a result of the compromise of their PII and/or PHI and remain at imminent risk that further compromises of their PII and/or PHI will occur in the future.

220. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant continues to owe a legal duty to secure current and former employees' PII and PHI, to timely notify current and former employees of any data breach,

and to establish and implement data security measures that are adequate to secure current and former employees' PII and PHI.

221. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect current and former employees' PII and PHI.

222. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury and lack an adequate legal remedy. The threat of another breach of the PII and/or PHI in Defendant's possession, custody, and control is real, immediate, and substantial. If another breach of Defendant's network, systems, servers, or workstations occurs, Plaintiff and Class members will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

223. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs at Defendant, Plaintiff and Class members will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

224. Issuance of the requested injunction will serve the public interest by preventing another data breach at Defendant, thus eliminating additional injuries to Plaintiff and the tens of thousands of Class members whose confidential information would be further compromised.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendant, as follows:

- A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;
- B. That Plaintiff be granted the declaratory relief sought herein;
- C. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;
- D. That the Court award Plaintiff and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;
- E. That the Court award Plaintiff and the Class members statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;
- F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;
- G. That the Court award pre- and post-judgment interest at the maximum legal rate;
- H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and
- I. That the Court grant all other relief as it deems just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a jury trial on all claims so triable.

Dated: October 20, 2021

Respectfully submitted,

/s/ Daniel O. Herrera

Daniel O. Herrera

Nickolas J. Hagman

**CAFFERTY CLOBES MERIWETHER  
& SPRENGEL LLP**

135 S. LaSalle, Suite 3210

Chicago, Illinois 60603

Telephone: (312) 782-4880

Facsimile: (312) 782-4485

dherrera@caffertyclobes.com

nhagman@caffertyclobes.com

Bryan L Clobes

**CAFFERTY CLOBES MERIWETHER  
& SPRENGEL LLP**

205 N. Monroe St.  
Media, Pennsylvania 19063  
Telephone: (215) 864-2800  
bclobes@caffertyclobes.com

# **EXHIBIT A**



Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

July 6, 2021



G5880-L01-0002755 T00012 P003 \*\*\*\*\*ALL FOR AADC 601

DOUGLAS J. MATTHEWS

BELLWOOD, IL



### Notice of Data Breach

Dear Douglas J Matthews:

Navistar, Inc. ("Navistar") values the privacy of our employees and uses physical, technical, and administrative measures to safeguard your personal information. We are writing to notify you about a security incident we recently experienced which has impacted your personal information. Below are details on the steps we are taking to address the situation, as well as what we are doing to support affected individuals.

#### WHAT HAPPENED?

On May 20, 2021, Navistar learned of a potential security incident affecting its information technology system ("IT System"). Upon learning of the security incident, Navistar launched an investigation and took immediate action in accordance with our cybersecurity response plan. Our investigation is ongoing with the assistance of leading cybersecurity experts hired to evaluate and address the scope and impact of the incident.

On May 31, 2021, Navistar received a claim that certain data had been extracted from our IT System. In the course of our investigation, we were able to confirm that an unauthorized third party had accessed and taken certain data from our IT System. On June 16, 2021, we discovered that some of the data taken by the unauthorized third party contains personal information about some of our current and former U.S. employees. Based on the information Navistar has at this time, we believe that this incident occurred prior to May 20, 2021 but our investigation is ongoing.

#### WHAT INFORMATION WAS INVOLVED?

The data that was taken included your full name, address, and social security number.

Navistar, Inc. 2701 Navistar Drive, Lisle, IL 60532 USA  
P : 331-332-5000 W : navistar.com

0002755



G5880-L01



**WHAT ARE WE DOING?**

We took immediate action to investigate the situation once we learned of the potential incident. Navistar has taken a number of steps to enhance our security protocols and controls, technology, and training. We continue to assess further options to protect our IT System.

Although we are not aware at this time that any third party has made any use of employee data as a result of this incident, out of an abundance of caution, we are providing you with access to free credit monitoring and identity theft protection for two years through Experian. Enrollment instructions and details for these free services are further outlined on Attachment 1.

**WHAT CAN YOU DO?**

In addition to using the credit monitoring and identity theft protection described above, we recommend that you remain vigilant for incidents of fraud and identity theft. You can review your account statements and monitor free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission ("FTC").

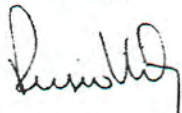
The FTC and the Internal Revenue Service ("IRS") both generally recommend that individuals who believe that they may be at risk of taxpayer refund fraud should file their income taxes as early as possible. The IRS further suggests that a taxpayer who is an actual or potential victim of identity theft complete and submit to the IRS Form 14039 (Identity Theft Affidavit). Form 14039 is available at <https://www.irs.gov/pub/irs-pdf/f14039.pdf>. Upon receipt of this affidavit, the IRS may flag your taxpayer account to identify questionable activity.

On behalf of Navistar, I want to apologize for any concern this situation may have caused. We appreciate the patience all our employees have demonstrated as we have worked to address this issue.

**FOR MORE INFORMATION.**

For more information and assistance, please contact (855) 387-4540 Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays).

Sincerely,



Persio V. Lisboa  
President & Chief Executive Officer

Attachment 1

**CREDIT MONITORING & IDENTITY THEFT PROTECTION SERVICES**

**Credit Monitoring Services Offer:**

We have retained Experian to assist us in providing you access to Experian IdentityWorks<sup>SM</sup>, its credit-monitoring service. Using Experian IdentityWorks, you can monitor your personal information. Experian IdentityWorks provides you with superior identity detection and resolution of identity theft.

**How to Enroll in Experian IdentityWorks and Activate Your Membership:**

You may enroll in and activate your complimentary two (2) year membership in Experian IdentityWorks by taking the following steps:

- **Visit the Experian IdentityWorks website** to enroll at:  
<https://www.experianidworks.com/3bcredit>
- **Activation Code.** Provide your activation code: [REDACTED]
- **Enroll by: September 30, 2021** (Your code will not work after this date.)
- **No Credit Card Required.** You do not need a credit card to enroll in Experian IdentityWorks.

**What if I Have Questions or Need Help Enrolling:**

If you have questions about Experian IdentityWorks or would like an alternative to enrolling online, please contact Experian's customer care team at (855) 387-4540 **by September 30, 2021**. Please be prepared to provide engagement number [REDACTED] as proof of eligibility.

**Can You Provide Me More Details Regarding My Membership?:**

Once you enroll in Experian IdentityWorks, you can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll:

- **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.



**What If I Believe That My Personal Information Has Been Used Without My Consent?**

Even if you do not enroll in Experian IdentityWorks, you are still automatically eligible to use Experian's Identity Restoration Services. Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time.

If you believe there was a fraudulent use of your personal information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

**What Else Can I Do to Protect My Personal Information?**

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information.

**ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT**

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

**Federal Trade Commission ("FTC")**

[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

*Take Charge: Fighting Back Against Identity Theft*

This is a comprehensive guide from the FTC to help you guard against and deal with identity theft

<https://www.identitytheft.gov/>.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

### Credit Bureaus

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at [www.annualcreditreport.com/manualRequestForm.action](http://www.annualcreditreport.com/manualRequestForm.action)

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
1-800-685-1111	1-888-397-3742	1-800-888-4213
<a href="http://www.equifax.com/CreditReport">www.equifax.com/CreditReport</a>	<a href="http://www.experian.com">www.experian.com</a>	<a href="http://www.transunion.com/fraud">www.transunion.com/fraud</a>
<u>Assistance</u>	P.O. Box 4500	P.O. Box 1000
P.O. Box 740241	Allen, TX 75013	Chester, PA 19016
Atlanta, GA 30374		

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

### **FOR MARYLAND RESIDENTS**

You can obtain information about preventing identify theft from the FTC or:

#### **Maryland Attorney General:**

Visit the Maryland Office of the Attorney General, Identity Theft Unit at:

<http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>

or call 410-576-6491

or write to this address:

Maryland Office of the Attorney General

Identity Theft Unit

16th Floor

200 St. Paul Place

Baltimore, MD 21202

### **FOR NORTH CAROLINA RESIDENTS**

You can obtain information about preventing identify theft from the FTC or:

#### **North Carolina Attorney General:**

Visit the North Carolina Office of the Attorney General at:

[www.ncdoj.gov](http://www.ncdoj.gov) or call 1-877-566-7226

or write to this address:

Attorney General's Office

9001 Mail Service Center

Raleigh, NC 27699-9001

0002755



G5880-L01

# **EXHIBIT B**



Return Mail Processing  
PO Box 999  
Suwanee, GA 30024

September 21, 2021

14 1 2802 \*\*\*\*\*AUTO\*\*ALL FOR AADC 601

DOUGLAS J. MATTHEWS



BELLWOOD, IL



Dear Douglas J. Matthews,

In early July of 2021, you should have received a letter from Navistar via First Class mail notifying you of a security incident involving the personal information of certain current and former U.S. employees. That notice included steps we've taken in response to the incident as well as what can be done to protect against any potential harm. That notice also provided you with additional information on how to access two years of free credit monitoring and identity theft protection, although we are not aware at this time that any third party has made any use of the affected data as a result of this incident.

After sending the July notification, we have continued to investigate the security incident and worked around the clock with the assistance of leading cybersecurity experts to confirm the full scope of the incident. We have now completed our investigation.

As a result of our investigation, we determined that some individuals who should have received the notification in July of 2021 (which stated that their name, address, and social security number were affected) also had certain information related to their participation in the Navistar health plan affected in the same security incident. You are one of those individuals.

As a result, we've enclosed a second letter to notify you that certain additional information related to your participation in the health plan was also affected in this incident. To be clear, this second letter is a result of our work to thoroughly investigate the incident, and **not** the result of a second incident.

Additional details regarding this incident, how you were affected, and how we are working to support you are included in the enclosed letter. Because you already should have received information regarding identity theft protection and the opportunity to enroll in credit monitoring services in your first letter, we are not including that information here. However, in case you have not yet enrolled in the credit monitoring services, we have extended the enrollment period until December 31, 2021 to allow you additional time to take advantage of that offering.

On behalf of Navistar, I want to assure you that we take the security of our systems and data very seriously and regret any concern this situation may have caused. We appreciate your patience as we have worked to address this issue.

Sincerely,



Donna Dorsey  
EVP, People & Culture  
Navistar, Inc.

Printed Name: Donna Dorsey  
Printed Title: EVP, People & Culture  
Printed Email: donna.dorsey@navistar.com



Dear Douglas J. Matthews,

In early July of 2021, you should have received a letter from Navistar as we were investigating a security incident involving the personal information of certain individuals and former UAW employees. The incident was caused by a third party who had access to our systems. As a result of this incident, we have taken steps to improve our security and protect your information. We have also provided you with a letter detailing the steps we have taken to address this issue.

After sending the July notification, we have continued to investigate the incident and have now completed our investigation. We have also updated our security protocols to prevent a similar incident from occurring in the future.

As a result of our investigation, we determined that the incident was caused by a third party who had access to our systems. We have taken steps to improve our security and protect your information. We have also provided you with a letter detailing the steps we have taken to address this issue.

As a result, we've enclosed a second letter to you regarding the incident. This letter provides additional information regarding the incident and the steps we have taken to address it. We have also provided you with a letter detailing the steps we have taken to address this issue.

Additional details regarding the incident have been provided to you in a separate letter. We have also provided you with a letter detailing the steps we have taken to address this issue. We have also provided you with a letter detailing the steps we have taken to address this issue.

Attachment 1

**ADDITIONAL INFORMATION ON CREDIT MONITORING & IDENTITY THEFT**

Individuals are advised to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports and to promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission.

The following are some resources:

**Federal Trade Commission ("FTC")**

[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

1-877-ID-THEFT (1-877-438-4338)

Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

*Take Charge: Fighting Back Against Identity Theft*

This is a comprehensive guide from the FTC to help you guard against and deal with identity theft

<https://www.identitytheft.gov/>.

**Credit Bureaus**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), calling 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at

[www.annualcreditreport.com/manualRequestForm.action](http://www.annualcreditreport.com/manualRequestForm.action)

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

<p><b>Equifax</b> 1-800-685-1111 <a href="http://www.equifax.com/CreditReportAssistance">www.equifax.com/CreditReport Assistance</a> P.O. Box 740241 Atlanta, GA 30374</p>	<p><b>Experian</b> 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a> P.O. Box 4500 Allen, TX 75013</p>	<p><b>TransUnion</b> 1-800-888-4213 <a href="http://www.transunion.com/fraud">www.transunion.com/fraud</a> P.O. Box 1000 Chester, PA 19016</p>
--	--	--

You can obtain additional information from the FTC and the nationwide credit reporting agencies about placing a security freeze on your credit files and fraud alerts. A security freeze is a free tool that lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. To place a security freeze on your credit files, contact each of the nationwide credit bureaus using the contact information listed above. You will need to supply your name, address, date of birth, social security number, and other personal information. You may want to consider placing a fraud alert on



your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information listed above.

Individuals are advised to remain vigilant in instances of fraud and identity theft by reviewing their credit reports and monitoring free credit reports to identify suspicious activity. Individuals should also be aware of the identity theft or other law enforcement agencies that may be contacted for assistance. Attorney General as well as the Federal Trade Commission.

The following are some resources:

Federal Trade Commission (FTC)  
www.ftc.gov/other  
1-877-FTC-HELP (3827)

Federal Trade Commission  
500 Pennsylvania Avenue NW  
Washington, DC 20580

For more information, visit the FTC's website at <https://www.ftc.gov>. This is a copy of the FTC's report on identity theft. For more information, visit the FTC's website at <https://www.ftc.gov>.

Credit Bureaus  
You may obtain a free copy of your credit report from each of the three major credit bureaus every 12 months by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com) or calling 1-877-839-8273. Credit Report request forms and mailing to Annual Credit Report Request Service, P.O. Box 1061, Atlanta, GA 30388. You can also obtain a copy of the report to [www.annualcreditreport.com](http://www.annualcreditreport.com).

Alternatively, you may elect to purchase a copy of your credit report or a copy of the credit report from a credit reporting agency. Contact information for the three major credit reporting agencies is listed below. The cost of purchasing a copy of your credit report or the cost of purchasing a copy of the credit report.

Equifax 1-800-888-1111 <a href="http://www.equifax.com/personal">www.equifax.com/personal</a> Atlanta, GA 30338 P.O. Box 740241	Experian 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a> P.O. Box 200 Allen, TX 75013	TransUnion 1-800-680-7273 <a href="http://www.transunion.com">www.transunion.com</a> P.O. Box 1348 Dunwoody, GA 30328
---	---	---

You can obtain additional information from the FTC and the three major credit bureaus by visiting [www.ftc.gov](http://www.ftc.gov) and [www.annualcreditreport.com](http://www.annualcreditreport.com). A security freeze on your credit file and a fraud alert are two different ways to protect access to your credit report, which is how thieves identify and steal your accounts in your name. To place a security freeze on your credit report, contact the credit bureau using the contact information listed above. You will need to identify your credit bureau and provide your social security number, and other personal information, to the credit bureau. You may want to consider placing a fraud alert on your credit report.



Return Mail Processing  
PO Box 999  
Suwanee, GA 30024

September 21, 2021

DOUGLAS J. MATTHEWS

BELLWOOD, IL

### Notice of Data Breach

Dear Douglas J. Matthews,

Navistar, Inc. ("Navistar") values the privacy of our current and former employees and uses physical, technical, and administrative measures to safeguard your personal information. Our records indicate you are a current or former participant in either the Navistar, Inc. Health Plan or the Navistar, Inc. Retiree Health Benefit and Life Insurance Plan (collectively, the "Plan"). We are writing to you to notify you about a security incident we recently experienced, which has impacted information related to your participation in the Plan. Below are details on the steps we are taking to address the situation.

#### WHAT HAPPENED?

On May 20, 2021, Navistar learned of a potential security incident affecting its information technology system ("IT System"). Upon learning of the security incident, Navistar launched an investigation and took immediate action in accordance with our cybersecurity response plan. Navistar conducted its investigation with the assistance of leading cybersecurity experts hired to evaluate and address the scope and impact of the incident.

On May 31, 2021, Navistar received a claim that certain data had been extracted from our IT System. In the course of our investigation, we were able to confirm that an unauthorized third party had accessed and taken certain data from our IT System, including data relating to participants in the Plan. On August 20, 2021, we discovered that some of the data taken by the unauthorized third party contains information relating to your participation in the Plan. Based on the information Navistar has at this time, we believe that this incident occurred prior to May 20, 2021.

#### WHAT INFORMATION WAS INVOLVED?

The data that was taken may have included your full name, address, date of birth, and information related to your participation in the Plan, such as information identifying certain of your providers and prescriptions.

#### WHAT ARE WE DOING?

We took immediate action to investigate the situation once we learned of the potential incident. Navistar has taken a number of steps to enhance our security protocols and controls, technology, and training. We continue to assess further options to protect our IT System.

**WHAT CAN YOU DO?**

We recommend that you remain vigilant for incidents of fraud and identity theft. You can review your account statements and monitor free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your bank or other financial institution holding your accounts, as well as any appropriate authorities, such as your state attorney general and the Federal Trade Commission ("FTC").

The FTC and the Internal Revenue Service ("IRS") both generally recommend that individuals who believe that they may be at risk of taxpayer refund fraud should file their income taxes as early as possible. The IRS further suggests that a taxpayer who is an actual or potential victim of identity theft complete and submit to the IRS Form 14039 (Identity Theft Affidavit). Form 14039 is available at <https://www.irs.gov/pub/irs-pdf/f14039.pdf>. Upon receipt of this affidavit, the IRS may flag your taxpayer account to identify questionable activity.

On behalf of Navistar, I want to apologize for any concern this situation may have caused. We appreciate the patience all our current and former employees have demonstrated as we have worked to address this issue.

**FOR MORE INFORMATION.**

For more information and assistance, please contact (855) 387-4540 Monday through Friday 8 am – 10 pm CST, Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays). Please be prepared to provide engagement number [REDACTED]

Sincerely,



Donna Dorsey  
EVP, People & Culture  
Navistar, Inc.

**FOR MARYLAND RESIDENTS**

You can obtain information about preventing identity theft from the FTC or:

**Maryland Attorney General:**

Visit the Maryland Office of the Attorney General, Identity Theft Unit at:

<http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>

or call 410-576-6491

or write to this address:

Maryland Office of the Attorney General

Identity Theft Unit

16th Floor

200 St. Paul Place

Baltimore, MD 21202

**FOR NORTH CAROLINA RESIDENTS**

You can obtain information about preventing identity theft from the FTC or:

**North Carolina Attorney General:**

Visit the North Carolina Office of the Attorney General at:

[www.ncdoj.gov](http://www.ncdoj.gov) or call 1-877-566-7226

or write to this address:

Attorney General's Office

9001 Mail Service Center

Raleigh, NC 27699-9001

**FOR RHODE ISLAND RESIDENTS**

Eight (8) individuals in Rhode Island were affected by this incident. You may obtain information about preventing identity theft from:

**Rhode Island Attorney General:**

Visit the Rhode Island Office of the Attorney General at:

[www.riag.ri.gov](http://www.riag.ri.gov), or call (401) 274-4400

or write to this address:

Rhode Island Office of the Attorney General

Consumer Protection Unit

150 South Main Street

Providence, RI 02903

**FOR WASHINGTON D.C. RESIDENTS**

You can obtain information about preventing identity theft from the FTC or the following:

**Washington D.C. Attorney General:**

Visit the Washington Office of the Attorney General (OAG) at:

<https://oag.dc.gov/>, or call the OAG's Office of Consumer Protection at 202-442-9828

or write to this address:

Office of the Attorney General

400 6th Street, NW

Washington, DC 20001

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Navistar Data Breach: Employee Alleges Hack Was 'Eminently Avoidable'](#)

---