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

THOMAS KALBRIER and CHERRIE KALBRIER, individually and on behalf of all others similarly situated, Plaintiffs, v. NAVISTAR, INC., Defendant.	CASE NO. Filed: October 1, 2021

CLASS ACTION COMPLAINT

Plaintiffs THOMAS KALBRIER and CHERRIE KALBRIER ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendant NAVISTAR, INC., ("Navistar" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyber-attack against Defendant Navistar that allowed a third party to access Defendant Navistar's computer systems and data, resulting in the compromise of highly sensitive personal information belonging to tens of thousands of current and former employees and their family members (the "Cyber-Attack").

2. As a result of the Cyber-Attack, Plaintiffs and Class Members suffered ascertainable injury and damages in the form of the substantial and present risk of fraud and identity theft from their unlawfully accessed and compromised private and confidential

information (including Social Security numbers), lost value of their private and confidential information, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

3. Plaintiffs' and Class Members' sensitive personal information—which was entrusted to Defendant, their officials and agents—was compromised, unlawfully accessed, and stolen due to the Cyber-Attack. Information compromised in the Cyber-Attack includes the following: names, Social Security numbers, driver's license numbers, and medical information (collectively the "Private Information").

4. Plaintiffs bring this class action lawsuit on behalf of all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

5. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant Navistar's computer network in a condition vulnerable to cyber-attacks of this type.

6. Upon information and belief, the mechanism of the Cyber-Attack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known and foreseeable risk to Defendant, and Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. The Cyber-Attack occurred prior to May 20, 2021, and was discovered on May 31, 2021. Had Defendant properly monitored their property, they would have discovered the intrusion sooner.

8. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

9. Armed with the Private Information accessed in the Cyber-Attack, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. As a further result of the Cyber-Attack, Plaintiffs and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

11. Plaintiffs and Class Members have and may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. As a direct and proximate result of the Cyber-Attack and subsequent Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer damages and economic losses in the form of: 1) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach; and 2) charges, and fees charged against their accounts. Plaintiffs and Class

Members have likewise suffered and will continue to suffer an invasion of their property interest in their own personally identifying information ("PII") such that they are entitled to damages for unauthorized access to and misuse of their PII from Defendant. And, Plaintiffs and Class Members will suffer from future damages associated with the unauthorized use and misuse of their PII as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

13. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or removed from the network during the Cyber-Attack.

14. Plaintiffs seek remedies including, but not limited to, compensatory damages, nominal damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Accordingly, Plaintiffs bring this action against Defendant seeking redress for their unlawful conduct asserting claims for negligence, negligence *per se*, and breach of implied contract.

PARTIES

16. Plaintiff Thomas Kalbrier is an individual citizen of the State of Oklahoma residing in Nowato, Oklahoma. Plaintiff Thomas Kalbrier was employed by Navistar as a customer service engineer from January 2005 to March 2015. Plaintiff Thomas Kalbrier received notice from Defendant that the Data Breach had occurred following a "security incident," and that his personal data (including his name, address date of birth, and Social Security number) was involved. A copy of the notice is attached hereto as **Exhibit A**.

17. Plaintiff Cherrie Kalbrier is an individual citizen of the State of Oklahoma residing in Nowato, Oklahoma. Plaintiff Cherrie Kalbrier was a participant in the Navistar, Inc. Health Plan. Plaintiff Cherrie Kalbrier received notice from Defendant that the Data Breach had occurred following a "security incident," and that her personal data (including her name, address date of birth, medical information) was involved. A copy of the notice is attached hereto as **Exhibit B**.

18. Defendant Navistar ("Navistar") is an Illinois corporation with its principal place of business at 2701 Navistar Drive, Lisle, Illinois, 60532.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and Plaintiffs Thomas Kalbrier and Cherrie Kalbrier and Members of the proposed Class are citizens of states different from Defendant.

20. The Northern District of Illinois has personal jurisdiction over Defendant because Defendant is headquartered in this District and Defendant conducts substantial business in Illinois and this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Business

22. Defendant Navistar is the parent company of International® brand commercial trucks and engines, IC Bus® brand school and commercial buses, OnCommand® Connection advanced connectivity services, aftermarket parts brands Fleetrite®, ReNEWed® and Diamond

Advantage® and Brazilian manufacturer of engines and gensets MWM Motores Diesel e Geradores. Navistar has more than 12,000 employees worldwide.[1]

23. In the ordinary course of doing business with Defendant, current and former employees provide Defendant with sensitive, personal and private information such as:

- Name;
- Address;
- Phone number;
- Driver's license number;
- Social Security number;
- Date of birth;
- Email address;
- Gender.

24. Current and former employees and their family members also participate in the Navistar, Inc. Health Plan and/or the Navistar, Inc. Retiree Health Benefit and Life Insurance Plan (the "Plans"). The Plans collect similar personal and private information from Plan participants. In addition, the Plans collect and maintain private health information ("PHI") from its participants.

25. Plaintiffs and Class Members, as current and former employees, or family members of current and former employees, relied on the Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

[1] https://www.navistar.com/about-us/our-company (last accessed Sept. 27, 2021).

26. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Cyber-Attack and Data Breach

27. On or about September 21, 2021, Defendant Navistar began notifying current and former employees, the family members of current and former employees, and state Attorneys General about a data breach that occurred prior to May 20, 2021 (the "Data Breach"). *See* Exhibits A and B, Plaintiffs' Notices of Data Breach.

28. According to the Notice of Data Breach letters, and letters sent to state Attorneys General, Navistar's security team, Navistar learned of a "potential security incident" on May 20, 2021, and on May 31, 2021, "received a claim that certain data had been extracted from our IT system." *Id.*

29. On June 7, 2021, Navistar disclosed in an 8-K SEC filing that it received a claim on May 31, 2021 that certain data had been extracted from the company's IT system.

30. On or about May 31, 2021, data stolen from Navistar was posted in Marketo, a "dark web" marketplace for stolen data.[2]

31. Plaintiff Thomas Kalbrier was informed that his name, address date of birth, and Social Security number may have been exfiltrated. *Id.*

32. Plaintiff Cherrie Kalbrier was informed that her name, address date of birth, and information related to her participation in the Plans, including medical information, may have been exfiltrated. *Id.*

[2] https://www.freightwaves.com/news/navistar-data-leaked-on-auction-site-after-cyberattack (last accessed Sept. 27, 2021).

33. The notice letters offered a "complementary two-year membership" to Experian IdentityWorksSM credit monitoring service.

34. Based on the Notice of Data Breach letters they received (Exhibits A and B to this Complaint), which informed Plaintiffs that their Private Information was accessed on Defendant's network and computer systems, and other publicly available information, Plaintiffs believe their name, address, date of birth and Social Security number were stolen from Defendant's network (and subsequently sold) on the Dark Web.

35. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

36. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

37. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

38. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[3]

39. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore,

[3] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 10, 2020).

the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

Defendant Fail to Comply with FTC Guidelines

40. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

41. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer 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 any security problems. 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.

42. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

43. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

44. Defendant failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

45. Defendant was at all times fully aware of its obligation to protect the PII and PHI of customers and prospective customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fail to Comply with Industry Standards

46. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

47. Best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

48. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7,

PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

49. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the Cyber-Attack and causing the data breach.

Defendant's Breach

50. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, networks, and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect current and former employees' Private Information;

c. Failing to adequately protect Private Information of current and former employees' family members;

d. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

e. Failing to apply all available security updates;

f. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

g. Failing to practice the principle of least-privilege and maintain credential hygiene;

h. Failing to avoid the use of domain-wide, admin-level service accounts;

i. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords; and

j. Failing to properly train and supervise employees in the proper handling of inbound emails.

51. As the result of computer systems in need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

Data Breaches Cause Disruption and Put Victims at an Increased Risk of Fraud and Identity Theft

52. Defendant was well aware that the Private Information it collected is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the cyber-criminals who perpetrated this Cyber-Attack.

53. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[4]

54. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven (7) years if

[4] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").

someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[5]

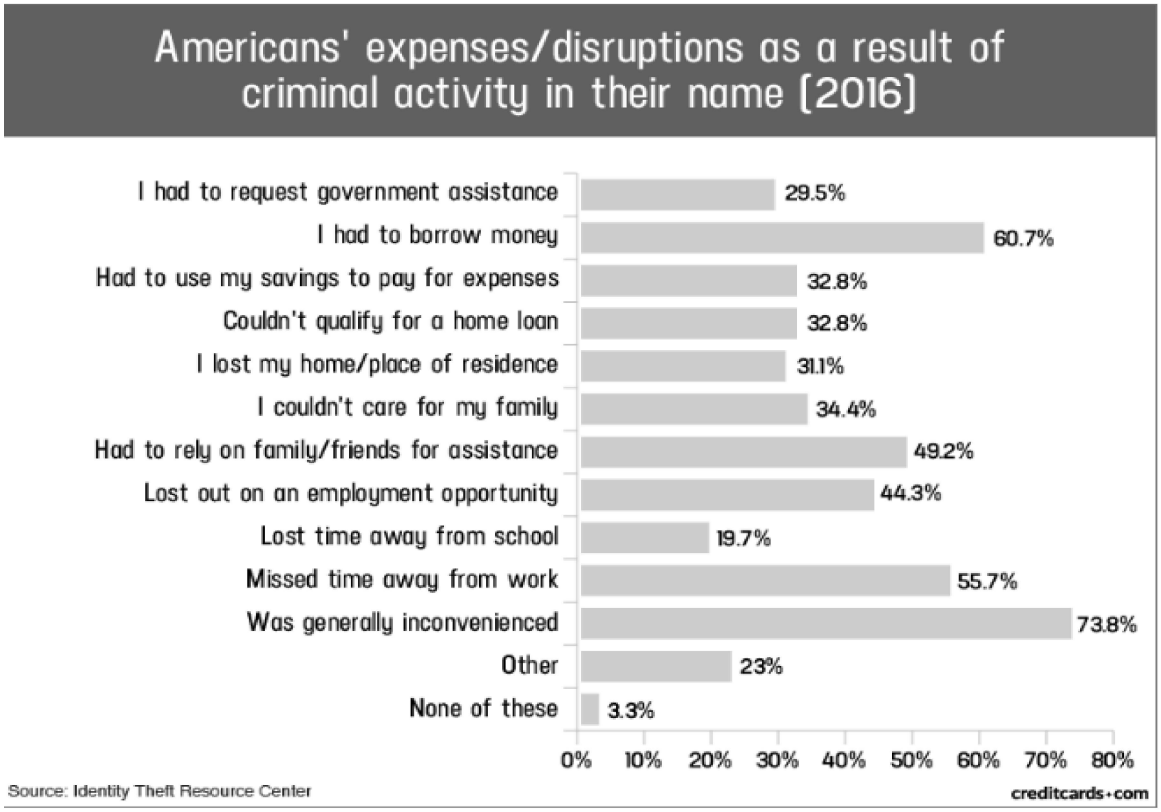
55. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

56. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

57. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

58. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[6]

[5] *See* https://www.identitytheft.gov/Steps (last visited Dec. 8, 2020).
[6] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last accessed Dec. 10, 2020).



59. What's more, theft of Private Information is also gravely serious. PII is a valuable property right.[7]

60. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

61. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[7] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report at 29.

62. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

63. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites.

64. Where the most private information belonging to Plaintiffs and Class Members was accessed and removed from Defendant's network, and entire batches of that stolen information already dumped by the cyberthieves on the cyber black market, there is a strong probability that additional batches of stolen information are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

65. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

66. Sensitive information can sell for as much as $363 according to the Infosec Institute. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

67. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.

68. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

69. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

70. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[8]

[8] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Oct. 28, 2020).

71. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[9]

72. At all relevant times, Defendant knew or reasonably should have known these risks, the importance of safeguarding Private Information, and the foreseeable consequences if its data security systems were breached, and strengthened their data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

Plaintiffs' and Class Members' Damages

73. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Cyber-Attack and data breach, including, but not limited to, the costs and loss of time they incurred because of the Cyber-Attack. Defendant has only offered 24 months of inadequate identity monitoring services, and it is unclear whether that credit monitoring was only offered to certain affected individuals (based upon the type of data stolen) or to all persons whose data was compromised in the Cyber-Attack.

74. Moreover, the 24 months of credit monitoring offered to persons whose private information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

[9] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 28, 2020).

75. Defendant entirely failed to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII.

76. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Cyber-Attack.

77. Plaintiff Thomas Kalbrier has suffered present injury in the form of the present, immediate, and continuing risk of harm through the theft of his name and Social Security number, which are the keys to financial fraud.

78. Plaintiffs have experienced an increase in spam texts and e-mails subsequent to the Data Breach that appear to have been placed with the intent to commit fraud or identity theft by way of a social engineering attack.

79. Plaintiffs and Class Members also face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

80. Plaintiffs and Class Members have been, and face substantial risk of being targeted in the future, subjected to phishing, data intrusion, and other illegal based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

81. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Cyber-Attack.

82. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Cyber-Attack. Numerous courts have recognized the propriety of loss of value damages in related cases.

83. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time (at least one hour per week) to monitor their financial accounts and records for misuse.

84. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Cyber-Attack. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Cyber-Attack relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

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

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

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

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

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

85. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

86. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

87. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

88. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

89. Plaintiffs bring this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to Federal Rule of Civil Procedure 23.

90. Plaintiffs propose the following Class definition(s), subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiffs bring this action and seeks certification of the following Class:

> All persons whose PII and/or PHI was compromised as a result of the Cyber-Attack that Navistar, Inc. discovered on or about May 20, 2021, and who were sent notice of the Data Breach.

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

91. Plaintiffs reserve the right to amend the definitions of the Class or add a Class if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

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

93. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of 112,116 of Defendant's current and former employees and Plan participants whose data was compromised in the Cyber-Attack and Data Breach.[10]

94. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

[10] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/1fbf84df-eb26-497d-b138-1a80b7cef361.shtml (63,126 persons affected) and https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (49,000 persons affected) (sites last visited Sept. 29, 2021).

a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Cyber-Attack;

c) Whether Defendant's data security systems prior to and during the Cyber-Attack complied with applicable data security laws and regulations;

d) Whether Defendant's data security systems prior to and during the Cyber-Attack were consistent with industry standards;

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

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

g) Whether computer hackers obtained Class Members' Private Information in the Cyber-Attack;

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

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

j) Whether Defendant's conduct was negligent;

k) Whether Defendant breach an implied contract between it and the Plaintiffs;

l) Whether Plaintiffs and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

95. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Cyber-Attack.

96. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class, and has no interests antagonistic to those of other Class Members. Plaintiffs' Counsel are competent and experienced in litigating data breach class actions.

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

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

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

CAUSES OF ACTION

COUNT I

NEGLIGENCE
(On Behalf of Plaintiffs and All Class Members)

100. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 99 above as if fully set forth herein.

101. Defendant required Plaintiffs and Class Members to submit non-public personal information as a condition of employment or to participate in the Plans.

102. By collecting and storing this data in its computer property, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

103. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

104. Defendant's duty of care to use reasonable security measures arose because Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

105. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

106. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Cyber-Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

107. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach

of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

108. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

109. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack and data breach.

110. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II

Negligence *Per Se*
(On Behalf of Plaintiffs and All Class Members)

111. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 99 above as if fully set forth herein.

112. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

113. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

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

115. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

116. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se.*

117. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

118. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

119. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and All Class Members)

120. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 99 above as if fully set forth herein.

121. Defendant required Plaintiffs and the Class to provide their personal information, including names, addresses, date of birth and Social Security numbers, as a condition of their employment and participation in the Plans.

122. As a condition of their employment with Defendant, Plaintiffs and the Class provided their personal and financial information. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

123. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

124. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal and financial information, including the personal information of their beneficiaries and dependents, and by failing to provide timely and accurate notice to them that personal and financial information, along with the personal information of their beneficiaries and dependents, was compromised as a result of the data breach.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

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

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

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

e) Ordering Defendant to pay for not less than five (5) years of credit monitoring services for Plaintiffs and the Class;

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

Dated: October 1, 2021

Respectfully submitted,

/s/ *Gary M. Klinger*
Gary M. Klinger
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (202) 429-2290
Fax: (202) 429-2294
gklinger@masonllp.com

Gary E. Mason
David K. Lietz
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Phone: (202) 429-2290
Fax: (202) 429-2294
dlietz@masonllp.com
gmason@masonllp.com

Attorneys for Plaintiffs and the Proposed Class