MICHAEL MANTAGAS and **MICHAEL ROBINA**, on behalf of themselves and all others similarly situated, Plaintiff, **v.** SHI INTERNATIONAL CORP. Defendant,	SUPERIOR COURT OF NEW JERSEY LAW DIVISION SOMERSET COUNTY Docket No.:_____ **CIVIL ACTION** **CLASS ACTION COMPLAINT** **JURY DEMAND**

Plaintiffs, MICHAEL MANTAGAS and MICHAEL ROBINA ("Plaintiffs"), individually and on behalf of the Class defined below of similarly situated persons, bring this action against Defendant SHI International Corp ("SHI" or "Defendant") to obtain damages, restitution, and injunctive relief from Defendant. Plaintiffs make the following allegations upon personal knowledge and belief, except as to their own actions, the investigation of counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") that was perpetrated against Defendant SHI, an international provider of information technology services, which held in its possession certain personally identifiable information ("PII") and private health information ("PHI") of Plaintiffs and the putative Class Members, who are (or were) employees of Defendant. As a result of the Data Breach, Plaintiffs and thousands of Class Members, suffered concrete injury in fact, including actual credit card fraud sustained by Plaintiff Robina.

2. In addition, Plaintiffs' and Class Members' sensitive personal information—which was entrusted to Defendant—was compromised and unlawfully accessed due to the Data Breach.

3. According to the Notice of Data Breach letter ("Notice") that Defendant sent to state Attorneys General, the private information compromised in the Data Breach included at least full names, Social Security numbers, home addresses, job titles, dates of employment, salary, tax, banking and loan information, and employees' COVID-19 vaccination status and dates of COVID-19 illness (collectively "Private Information").[1]

4. The Private Information compromised in the Data Breach was exfiltrated by the cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect employees' Private Information.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Due to Defendant's status as a provider of IT products and services, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant and Defendant was thus on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. Defendant disregarded the rights of Plaintiffs and Class Members by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent

[1] https://www.mass.gov/doc/assigned-data-beach-number-27957-shi-international-corp/download

the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

8. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner or prevented it entirely.

9. 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.

10. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud (including the credit card fraud suffered by Plaintiff Robina described below), and can in the future 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' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims 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.

11. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent 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.

12. Plaintiffs and Class Members 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.

13. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiffs seek remedies including, but not limited to, compensatory 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 its unlawful conduct.

PARTIES

16. Plaintiff Michael Mantagas is, and at all times mentioned herein was, an individual citizen of the State of New Jersey, residing in the city of Manalapan. Plaintiff Mantagas is a former employee of SHI. As a condition of Plaintiff Mantagas' employment at SHI, he was required to and did provide his Private Information to Defendant. Plaintiff Mantagas received notice of the Data Breach on or about July 27, 2022.

17. Plaintiff Michael Robina is, and at all times mentioned herein was, an individual citizen of the State of New Jersey, residing in the city of Chatham. Plaintiff Robina is a former employee of SHI. As a condition of Plaintiff Robina's employment at SHI, he was required to and did provide his Private Information to Defendant. Plaintiff Robina received notice of the Data Breach on or about July 27, 2022.

18. Defendant SHI is a corporation organized under the laws of the State of New Jersey, with a principal place of business at 290 Davidson Ave, Somerset, NJ 08873.

JURISDICTION AND VENUE

19. This Court has personal jurisdiction over Defendant because it regularly conducts substantial business in New Jersey, has its principal place of business located in New Jersey and the amount in question in this litigation is greater than $15,000.

20. Venue is proper in Somerset County under R. 4:3-2(b) as Defendant conducts substantial business throughout Somerset County and has its principal place of business in Somerset County.

FACTUAL ALLEGATIONS

A. *Defendant's Business*

21. Defendant is an international provider of IT services to more than 15,000 private sector businesses, public sector entities, and academic organizations. In 2021, Defendant generated $12.3 billion in revenue, and employed 5,000 individuals in the U.S., the United Kingdom, and the Netherlands.[2]

22. SHI International offers the full spectrum of IT solutions including IT lifecycle services, data centers, cloud computing, data management, professional and technical training, digital infrastructure, and most pertinently, cybersecurity solutions:

[2] https://www.businesswire.com/news/home/20220307005630/en/%C2%A0SHI-International-Earns-Record-12.3-Billion-in-2021-Revenue-Up-10-Year-Over-Year

23. Defendant's webpage is replete with warnings regarding the frequency and severity of cyberattacks and the consequences that result from failures to implement proper data security practices.[3] Defendant admonishes potential customers that "your digital assets are subject to constant attacks. The average cost to businesses affected by data breaches is estimated at $3.86 million, making cybersecurity a priority."

24. Defendant similarly acknowledges the need for companies to protect employees in addition to company assets and offers "expert services help ensure your infrastructure, data and people are protected as cybersecurity threats and the regulatory landscape change."

25. Unfortunately for SHI's employees, like Plaintiffs and Class Members, SHI failed to adequately protect their Private Information from threats known to and anticipated by it.

26. In the course of collecting Private Information from employees, including Plaintiffs, SHI promised, directly or indirectly, to provide confidentiality and adequate security for employee data.

27. On information and belief, SHI made these promises in, among other things, its privacy notices that are made available to employee candidates in the course of their employment enrollment process.

28. Plaintiffs and the Class Members, as former and current SHI employees and employee candidates, relied on these implicit and express promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Employees, in general, demand security to safeguard their Private Information,

[3] https://www.shi.com/solutions/cybersecurity

especially when Social Security numbers, salaries, health information, and other sensitive data is involved, as here.

29. In the course of their employment relationship, employees, including Plaintiffs and Class Members, provided SHI with at least the following Private Information:

a. names;

b. dates of birth;

c. Social Security numbers;

d. driver's license number;

e. medical information; and

f. health insurance information.

30. SHI also aggregated and maintained information developed during the course of the employment relationship like job titles, dates of employment, salary, tax, and banking and loan information.

31. Due to the sensitivity of the information and the fact that SHI alone was in a position to safeguard it, SHI had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from involuntary disclosure to third parties.

B. *The Data Breach*

32. In the Notice letters sent to Plaintiffs and Class Members on July 27, 2022, Defendant SHI admits that it discovered "unauthorized access to its computer systems" and that employee data was "compromised." SHI further admits that it "is implementing heightened security measures to further protect your information and the integrity of our systems and operations."[4]

[4] *See* Notice

33. As evidenced by their receiving Notice letters, Plaintiffs' and Class Members' information was in fact involved in the data security incident.

34. SHI disclosed the Data Breach's occurrence on July 6, 2022 but did not begin noticing Plaintiffs and Class Members until July 27, 2022.[5]

35. SHI publicly confirmed that it "was the target of a coordinated and professional malware attack," and acknowledged its duty to prevent the Data Breach in stating "[t] he security and integrity of SHI's systems – and, by extension, the security of our customers – is paramount to SHI.[6]

36. Nonetheless, SHI allowed unauthorized criminal actors to access the Private Information of Plaintiffs' and Class Members and similarly allowed those actors to hijack and take offline its systems through a malware attack. SHI's website remained offline through July 7, 2022.[7]

37. Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid. While at one time the prime motive of a ransomware attack was simply to encrypt a user's data and hold it for ransom, ransomware attacks are now primarily the last phase of a multi-pronged cyberattack that is targeted at confidential data, and that has as its prime motivation the theft of confidential data like the Social Security numbers stolen here. A recent analysis shows that data exfiltration occurs in 70% of all ransomware attacks.[8]

---

[5] *See* Recent Security Incident: Statement from SHI available at https://blog.shi.com/uncategorized/recent-security-incident-statement-from-shi (last visited on Aug. 17, 2022).
[6] *Id.*
[7] *Id.*
[8] Jessica Davis, *70% Ransomware Attacks Cause Data Exfiltration; Phishing Top Entry Point*, HealthITSecurity (Feb. 3, 2021), https://healthitsecurity.com/news/70-ransomware-attacks-cause- data-exfiltration-phishing-top-entry-point.

38. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as an international IT provider and employer that collects, creates, and maintains particularly sensitive Private Information.

39. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from SHI that included the Private Information of Plaintiffs and Class Members.

40. The files stolen from SHI contained at least the following information of Plaintiffs and Class Members: full names, Social Security numbers, home addresses, job titles, dates of employment, salary, tax, banking and loan information, and employees' COVID-19 vaccination status and dates of COVID-19 illness.

41. As a result of the Data Breach, SHI informed Plaintiffs and Class Members to "remain vigilant by reviewing account statements and monitoring free credit reports for incidents of fraud and identity theft. . ."[9]

42. That SHI is encouraging its employee applicants, current employees and former employees to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted consumers are subject to a substantial and imminent threat of fraud and identity theft.

43. SHI could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

44. The Private Information contained in SHI's network was not encrypted because if it were, Plaintiff Robina and other members of the Class would not have experienced attempts at fraud since the Data Breach. Specifically, Plaintiff Robina had his credit card information used to make fraudulent charges.

[9] *Id.*

45. SHI had obligations created by contract, industry standards, and common law to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

46. SHI also failed to give timely and accurate notice of the Data Breach. SHI admits that the breach was discovered on July 4, 2021, and notice was not sent out until July 27, 2022.[10] Moreover, while SHI contends that Plaintiffs' and Class Members' information "may" have been among the compromised data, that contention is belied by the fact of sending formal notice of the data breach, which is generally only required when this is more than a low probability that protected information was compromised. SHI's notice is therefore misleading and incomplete, when it knows with reasonable certainty that Plaintiffs' and Class Members' Private Information was accessed.

47. SHI's notice is further incomplete and misleading as it does not disclose the specific information pertaining to each Class Member that was accessed in the Data Breach, the precise means of the attack, and whether Plaintiffs' and Class Members Private Information is still in the hands of the attackers.

Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' PII.

48. SHI acquires, collects, and stores a massive amount of PII on its employees, former employees and other personnel.

49. As a condition of employment, or as a condition of receiving certain benefits, SHI requires that employees, job applicants, and other personnel entrust it with highly sensitive personal information.

[10] *Id.*

50. By obtaining, collecting, and using Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

51. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

52. Plaintiffs and the Class Members relied on 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.

The Ransomware Attack and Data Breach were Foreseeable Risks of which Defendant was on Notice

53. It is well known that Private Information, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

54. Individuals place a high value not only on their Private Information, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

55. Individuals are particularly concerned with protecting the privacy of their Social Security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." These are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."

56. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[11]

57. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), SHI knew or should have known that its electronic records would be targeted by cybercriminals.

58. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

59. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, SHI failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

At All Relevant Times SHI had a Duty to Plaintiffs and Class Members to Properly Secure their Private Information.

60. At all relevant times, SHI had a duty to Plaintiffs and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to promptly notify Plaintiffs and

[11] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com /tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/.

Class Members when SHI became aware that their Private Information may have been compromised.

61. SHI's duty to use reasonable security measures arose as a result of the special relationship that existed between SHI, on the one hand, and Plaintiffs and the Class Members, on the other hand. The special relationship arose because Plaintiffs and the Members of the Class entrusted SHI with their Private Information as a condition of their employment with SHI and they relied on SHI to keep that Private Information secure.

62. SHI had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures commensurate with the foreseeable risk involved, despite its obligation to protect such information. Accordingly, SHI breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

63. Security standards commonly accepted among businesses that store Private Information using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for Private Information;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

64. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[13]

65. The ramifications of SHI's failure to keep its employees' Private Information secure are long lasting and severe. Once Private Information is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims may continue for years.

The Value of Personal Identifiable Information.

66. The Private Information 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. [14]

67. Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

[12] 17 C.F.R. § 248.201 (2013).
[13] *Id.*
[14] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark- web-how-much-it-costs/.
[15] *In the Dark*, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in- the-dark/.

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

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

69. What's more, it is no 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. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

70. 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."[17]

---

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[17] 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.

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."[17]

72. Private Information can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[18]

73. Given the nature of the Data Breach, it is foreseeable that the compromised Private Information can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class Members' Private Information can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

74. The information compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

75. To date, SHI has offered its employees, whose data was compromised, only two years of credit monitoring. The offered services are inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here.

76. The injuries to Plaintiffs and Class Members were directly and proximately caused by SHI's failure to implement or maintain adequate data security measures for its current and former employees.

[18] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1

Defendant Fails to Comply with FTC Guidelines.

77. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business 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.[19]

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.[20] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as 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.

79. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[21]

80. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

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

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

---

[19] Federal Trade Commission, *Start With Security*, *available at*: https://www.ftc.gov/system/files /documents/plain-language/pdf0205-startwithsecurity.pdf.
[20] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide- business.
[21] FTC, *Start With Security*, *supra* note 18.

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

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

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

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

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

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

81. The FTC has brought enforcement actions against businesses for failing to protect consumer and 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.

82. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

83. Because Class Members entrusted SHI with their Private Information, SHI had, and has, a duty to the Class Members to keep their Private Information secure.

84. Plaintiffs and the other Class Members reasonably expected that when they provide Private Information to SHI, SHI would safeguard their Private Information.

85. SHI was at all times fully aware of its obligation to protect the personal and financial data of employees, including Plaintiffs and Members of the Class. SHI was also aware of the significant repercussions if it failed to do so.

86. SHI's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiffs' and Class Members' Social Security numbers, driver's license numbers, financial account information, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standard.

87. Several best practices have been identified that at a minimum should be implemented by companies like Defendant SHI, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

88. Other best cybersecurity practices that are standard in the healthcare 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; and training staff regarding critical points.

89. Defendant failed to meet the minimum standards of any of the following 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 all established standards in reasonable cybersecurity readiness.

90. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant breached its obligations to its current and former employees.

91. Defendant breached its obligations to Plaintiff and the members of the Class or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, networks, and data.

92. Defendant's unlawful conduct includes, but is not limited to, the following acts 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.

93. Because Defendant needed to upgrade its computer systems' security and its procedures for handling cybersecurity threats, and it did not do so, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class members' Private Information.

Plaintiffs and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security and The Data Breach It Allowed.

94. Plaintiffs and Class Members reasonably expected that Defendant would provide adequate security protections for their Private Information, and Class Members provided Defendant with sensitive personal information, including their Social Security numbers, health insurance information and driver's license numbers.

95. Defendant' s poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to employment with Defendant, Plaintiffs and other reasonable former and current employees understood and expected that, as part of that employment relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiffs and the Class Members suffered pecuniary injury.

96. Cybercriminals capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiffs have also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of responding to the Data Breach including engaging adequate credit monitoring and identity theft protection services.

97. The cybercriminals who obtained the Class Members' Private Information may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

a. obtaining employment;

b. obtaining a loan;

c. applying for credit cards or spending money;

d. filing false tax returns;

e. stealing Social Security and other government benefits; and

f. applying for a driver's license, birth certificate, or other public document.

98. Additionally, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

99. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and the other Class Members have been deprived of the value of their PII, for which this is a well-established national and international market.

100. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[22]

101. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[23] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[24] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places

[22] *Id.*
[23] *Data Breach Victims More Likely To Suffer Identity Fraud*, Insurance Information Institute Blog (Feb. 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267.
[24] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php.

consumers at a substantial risk of fraud."[25] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

102. As a result of the Data Breach, Plaintiffs and Class Members have already suffered damages.

103. Defendant openly admits that the cybercriminals coordinated to conduct a "professional malware attack" and that a trove of Private Information concerning Plaintiffs' and the Class was "compromised."

Plaintiffs' and Class Members' Damages

104. To date, Defendant has not provided Plaintiffs and the members of the Class with adequate 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.

105. Specifically, Defendant has only offered two years of credit monitoring to persons whose Private Information was compromised in the Data Breach.

106. Moreover, the offered service 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.

107. Defendant did not provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class members' Private Information despite advising Plaintiffs and

[25] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, *available at* https://www.it.northwestern.edu /bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf.

Class Members to take affirmative steps to protect themselves from the consequences of the Data Breach.

108. Plaintiffs and the members of the Class have been damaged by the compromise of their Private Information in the Data Breach.

109. Moreover, Defendant's delay in noticing affected persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

Plaintiff Mantagas' Experience

110. Prior to the Data Breach, Plaintiff Mantagas was employed at SHI. In the course of enrolling in employment with SHI and as a condition of continued employment, he was required to supply SHI with his Private Information. Plaintiff Mantagas received the Notice Letter on or about July 27, 2021.

111. Subsequent to the Data Breach, Plaintiff Mantagas experienced an increase in the number of spam phone calls, emails and texts, in particular emails related to payday loans. As a result of the Data Breach, Plaintiff Mantagas has spent time dealing with these suspicious communications and monitoring his financial accounts for suspicious activity.

112. In response to the Data Breach, Plaintiff Mantagas spent time dealing with the consequences of the Data Breach, which included and will include time spent verifying the legitimacy of the Notice, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

113. Plaintiff Mantagas is very careful about sharing Private Information and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

114. Plaintiff Mantagas stores any documents containing Private Information in a safe and secure location and shreds any documents he receives in the mail that contain any Private

Information, or that may contain any information that could otherwise be used to compromise his credit card accounts and identity. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

115. Plaintiff Mantagas suffered actual injury and damages as a result of the Data Breach. Implied in his employment contract with SHI was the requirement that it adequately safeguard his Private Information. Plaintiff Mantagas would not have worked for SHI or would not have provided his Private Information had SHI disclosed that it lacked data security practices adequate to safeguard Private Information.

116. Plaintiff Mantagas suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to SHI for the purpose of employment, which was compromised by the Data Breach.

117. Plaintiff Mantagas suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

118. Plaintiff Mantagas has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

119. Plaintiff Mantagas has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in SHI's possession, is protected and safeguarded from future breaches.

Plaintiff Robina's Experience

120. Prior to the Data Breach, Plaintiff Robina was employed at SHI. In the course of enrolling in employment with SHI and as a condition of continued employment, he was required to supply SHI with his Private Information. Plaintiff Robina received the Notice Letter on or about July 27, 2021.

121. Subsequent to the Data Breach, Plaintiff Robina's credit card information was used to make fraudulent charges. As a result of the Data Breach, Plaintiff Robina has spent time dealing with these charges and monitoring his financial accounts for suspicious activity.

122. In response to the Data Breach Plaintiff Robina spent time dealing with the consequences of the Data Breach, which included and will include time spent verifying the legitimacy of the Notice, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

123. Plaintiff Robina is very careful about sharing Private Information and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

124. Plaintiff Robina stores any documents containing Private Information in a safe and secure location and shreds any documents he receives in the mail that contain any Private Information, or that may contain any information that could otherwise be used to compromise his credit card accounts and identity. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

125. Plaintiff Robina suffered actual injury and damages as a result of the Data Breach. Implied in his employment contract with SHI was the requirement that it adequately safeguard his Private Information. Plaintiff Robina would not have worked for SHI or would not have provided

his Private Information had SHI disclosed that it lacked data security practices adequate to safeguard Private Information .

126. Plaintiff Robina suffered actual injury in the form fraudulent charges to his credit card as well as damages and diminution in the value of his Private Information —a form of intangible property that he entrusted to SHI for the purpose of employment, which was compromised by the Data Breach.

127. Plaintiff Robina suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

128. Plaintiff Robina has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information , especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

129. Plaintiff Robina has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in SHI's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

130. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

131. Plaintiffs proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was maintained on Defendant SHI's computer systems that were compromised in the Data Breach, and who were sent Notice of the Data Breach.

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

133. Plaintiffs hereby reserve the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

134. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the 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.

135. **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 at least 11,000 persons whose data was compromised in Data Breach.

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

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

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

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

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

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

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

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

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 breached implied contracts for adequate data security with Plaintiffs and Class Members;

l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiffs and Class Members;

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

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

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

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

139. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' Private Information 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.

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

141. 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.

142. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

134. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of Data Breach by Defendant.

COUNT I
Negligence
(on behalf of Plaintiffs and all Class Members)

143. Plaintiffs re-allege and incorporate by reference the above allegations as if fully set forth herein.

144. Defendant required Plaintiffs and Class Members to submit non-public Private Information as a condition of employment or as a condition of receiving employee benefits.

145. Plaintiffs and the Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information.

146. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

147. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII 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.

148. 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.

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

150. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against.

151. 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 members of the Class.

152. Defendant breached its duties to Plaintiffs and the members of the Class 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.

153. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

154. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. 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. Failing to periodically ensure that their email 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; and

f. Failing to delete or destroy the Private Information of former employees or applicants that it was no longer required to maintain for business or legal reasons.

155. 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 industry.

156. 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.

157. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the Private Information and the harm suffered, or risk of imminent harm suffered by Plaintiffs and the Class.

158. As a result of Defendant's negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: fraudulent charges to their credit cards; out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

159. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

160. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its 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
Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

161. Plaintiffs re-allege and incorporate by reference the above allegations as if fully set forth herein.

162. Plaintiffs and Class Members were required to and did provide their Private Information to Defendant as a condition of their employment with Defendant.

163. Plaintiffs and Class Members provided their labor and Private Information to Defendant in exchange for (among other things) Defendant's promise to protect their PII from unauthorized disclosure.

164. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

165. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

166. Implicit in the agreement between Plaintiffs and Class Members and Defendant to provide Private Information , was the latter' s obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that Private Information , (c) prevent unauthorized disclosures of the Private Information , (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e)

reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential and only to the extent neccesary.

167. When Plaintiffs and Class Members provided their PII to Defendant as a condition of their employment or employee beneficiary status, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

168. Defendant required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

169. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

170. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

171. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

172. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

173. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

174. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

175. Plaintiffs and Class Members are also entitled to nominal damages for the breach of implied contract.

176. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and all Class Members)

177. Plaintiffs re-allege and incorporate by reference the above allegations as if fully set forth herein.

178. Plaintiffs allege this Count (unjust enrichment) solely in the alternative to Count II (breach of implied contract) above.

179. Plaintiffs and Class Members conferred a monetary benefit on Defendant by providing Defendant with their labor and Private Information.

180. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

181. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant

instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

182. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

183. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

184. If Plaintiffs and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

185. Plaintiffs and Class Members have no adequate remedy at law. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information ; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information ; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in

terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

186. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

187. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

COUNT IV
Invasion of Privacy
(On Behalf of Plaintiffs and All Class Members)

188. Plaintiffs re-allege and incorporate by reference the above allegations as if fully set forth herein.

189. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to and access by unauthorized third parties.

190. Defendant owed a duty to its students, employees, and independent contractors, including Plaintiff and the Class, to keep this information confidential.

191. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' Private Information is highly offensive to a reasonable person.

192. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant to receive trucking training services and employment, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff

and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

193. Had Plaintiffs and members of the Class known that Defendant would not adequately protect their PII, Plaintiffs and members of the Class would not have entrusted Defendant with their Private Information.

194. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

195. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

196. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

197. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

198. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

199. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

200. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages alone will not end Defendant's inability to safeguard the Private Information of Plaintiff and the Class.

201. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other members of the Class, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs in addition to all other damages or relief allowed by law.

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. or 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 Private Information 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 lifetime credit monitoring services for Plaintiffs and the Class;

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

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

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

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

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

JURY DEMAND

Plaintiffs demand a trial by jury on all triable issues.

DATED: August 24, 2022

/s/ Victoria Maniatis
Victoria Maniatis
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza
Suite 500
Garden City, NY 11530
Tel: 516-741-5600
Vmaniatis@milberg.com

David K. Lietz (*pro hac vice forthcoming*)
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20016
Phone: 866.252.0878
dlietz@milberg.com

ClassAction.org
