CHAFFIN LUHANA LLP
Roopal P. Luhana, Esq.
Steven D. Cohn, Esq. (*pro hac vice forthcoming*)
600 3rd Avenue, 12th Floor
New York, New York 10016
(888) 480-1123 telephone
(888) 499-1123 facsimile
luhana@chaffinluhana.com
cohn@chaffinluhana.com

MASON LIETZ & KLINGER LLP
Gary M. Klinger (*pro hac vice* forthcoming)
221 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: (202) 975-0477
gklinger@masonllp.com

Attorneys for Plaintiff and
the Proposed Class

EDWARD GONSHOROWSKI, on behalf of himself and all others similarly situated,	**: SUPERIOR COURT OF NEW JERSEY** **: LAW DIVISION:** **: ATLANTIC COUNTY**
Plaintiffs,	**:DOCKET NO.:**
v.	**:CIVIL CLASS ACTION**
SPENCER GIFTS LLC,	**:CLASS ACTION COMPLAINT &** **:JURY DEMAND**
Defendant.	

CLASS ACTION COMPLAINT

1. Plaintiff, EDWARD GONSHOROWSKI ("Plaintiff") brings this Class Action Complaint against Spencer Gifts LLC ("Defendant" or "SGL") in their individual capacity and on behalf of all others similarly situated (the "Class," defined below), and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows.

JURISDICTION AND VENUE

2. This is an action for damages that exceed the jurisdictional minimum of this Court.

3. Venue is proper in this County pursuant to Rule 4:3-2 in that Defendant resides in Atlantic County, New Jersey.

4. Venue is proper in this County pursuant to Rule 4:3-2 in that Defendant does substantial business in Atlantic County, New Jersey.

NATURE OF THE ACTION

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

6. As a result of the Cyber-Attack, Plaintiff 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 and financial account 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.

7. Plaintiff's 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: full name, Social Security number, health plan selection, and financial account numbers used for direct deposit (collectively the "Private Information").

8. Plaintiff brings 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.

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

10. Upon information and belief, the mechanism of the Cyber-Attack and potential for improper disclosure of Plaintiff's 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.

11. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored their property, they would have discovered the intrusion sooner.

12. Plaintiff's 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.

13. 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' 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.

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

15. Plaintiff 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.

16. As a direct and proximate result of the Cyber-Attack and subsequent Data Breach, Plaintiff 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. Plaintiff 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 Plaintiff 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.

17. Plaintiff seeks 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.

18. Plaintiff seeks 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.

19. Accordingly, Plaintiff brings this action against Defendant seeking redress for their unlawful conduct asserting claims for negligence, negligence per se, and breach of implied contract.

PARTIES

20. Plaintiff EDWARD GONSHOROWSKI is an individual citizen of the State of California residing in West Covina, California. Plaintiff Gonshorowski was last employed by SGL in or around 2009. On or about January 21, 2022, Plaintiff Gonshorowski received notice from Defendant that the Data Breach had occurred following a security "incident," and that his personal data (including his name and Social Security number and financial account number) was involved.

21. Defendant Spencer Gifts LLC ("SGL") is a New Jersey limited liability company with its principal place of business in Egg Harbor Township, New Jersey.

FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

22. Defendant SGL is a North American mall retailer with over 600 stores in the United States and Canada. Their stores specialize in novelty and gag gifts, and also sell

clothing, band merchandise, room decor, collectible figures, fashion and body jewelry, fantasy and horror items.

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;
- Account Number; and/or
- Credit / Debit Card Number (in combination with security code, access code, password or PIN for the account.

24. Plaintiff and Class Members, as 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. Plaintiff and Class Members demand security to safeguard their PII.

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

The Cyber-Attack and Data Breach

26. On January 24, 2022, Defendant SGL began notifying current and former employees and state Attorneys General about a data breach that occurred in November 2021 (the "Data Breach").

27. According to the Notice of Data Breach letter and letters sent to state Attorneys General, SGL detected a security incident on November 25, 2021. Upon discovering the incident, SGL notified law enforcement and began an investigation. Through the investigation, SGL

determined that an unauthorized actor accessed its network between November 24, 2021 and November 26, 2021, including certain files contained on its servers. *Id.*

28. SGL reviewed those files and identified documents relating to payroll and enrollment in its employee health plan. These documents contained individuals' names, Social Security Numbers, health plan selection, and financial account numbers used for direct deposit.

29. Plaintiff was informed that his full name, Social Security Number, health plan selection, and financial account number used for direct deposit was compromised. *Id.*

30. The notice letters offered a complementary twelve-month membership to Experian's Identity Works credit monitoring service.

31. Based on the Notice of Data Breach letters he received, which informed Plaintiff that his Private Information was accessed on Defendant's network and computer systems, and other publicly available information, Plaintiff believes his Private Information was stolen from Defendant's network and subsequently sold on the Dark Web.

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

33. Plaintiff 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.

34. 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.

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

36. 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, 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.

Plaintiff's Exposure and Mitigation Efforts

37. As a direct result of the Data Breach, Plaintiff has engaged in mitigation efforts and expended time and resources.

38. Subsequent to the Breach, Plaintiff experienced an increase in spam phone calls and emails to the phone number and email account he provided to Defendant. The calls and emails appear to be placed with the intent of obtaining personal information to commit identity theft by way of a social engineering attack.

39. Subsequent to the Breach, Plaintiff now regularly checks his credit reports as well as his banking statements and credit card statements several times a week. In fact, following the Breach, Plaintiff was kept on hold with his bank for approximately 4 hours trying to determine if his PII was misused as a result of the Breach. This is time Plaintiff otherwise would have spent performing other activities, such as his working or leisure activities.

40. Knowing that thieves stole his PII and knowing that this information may now, or in the future, be available for sale on the dark web has caused Plaintiff anxiety. He is now very

[1] 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).

concerned about identity theft in general. This Data Breach has given Plaintiff hesitation about using electronic services and reservations about conducting other online activities requiring his PII.

41. Prior to receiving the notice letter from Defendant, Plaintiff had not received a notice of data breach letter from any other company.

42. Plaintiff suffered actual injury from having his PII exposed as a result of the Data Breach including, but not limited to: (a) entrusting his PII to SGL which he would not have, had SGL disclosed that it lacked data security practices adequate to safeguard consumers' PII from theft; (b) damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to SGL as a condition of employment; (c) loss of his privacy; (d) present injury arising from the increased risk of fraud and identity theft; and (e) the time and expense of his mitigation efforts as a result of the Data Breach.

43. As a result of the Data Breach, Plaintiff will continue to be at a substantial and present risk for financial fraud and identity theft, and the attendant damages, for years to come.

Defendant Failed to Comply with FTC Guidelines.

44. The Federal Trade Commission ("FTC") promulgates numerous guides for businesses highlighting 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.[2]

[2] Federal Trade Commission, *Start With Security*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Sept. 9, 2021).

45. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[3] The guidelines note that businesses should protect the personal customer information they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

46. The FTC further recommends 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 third–party service providers have implemented reasonable security measures.[4]

47. The FTC brings enforcement actions against businesses for failing to adequately and reasonably protect customer data, 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.

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

---

[3] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Sept. 9, 2021).

[4] FTC, *Start With Security*, *supra* note 17.

49. Defendant was at all times fully aware of its obligation to protect Plaintiff's and Class members' PII because of Defendant's position as Plaintiff's and Class members' employer. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards.

50. 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.

51. 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.

52. 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.

53. 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

54. Defendant breached its obligations to Plaintiff 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.

55. 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 Plaintiff's and Class Members' Private Information.

Data Breaches Put Victims at a Present Increased Risk of Fraud and Identity Theft

56. Defendant understood 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.

57. 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."[5]

58. 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 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.[6]

59. 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.

60. 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

[5] *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").
[6] *See* https://www.identitytheft.gov/Steps (last visited Dec. 8, 2020).

and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

61. 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.

62. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[7]

63. The value of personal data 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.

64. 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:

> [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.

[7] *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).

65. 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.

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

67. Where the most private information belonging to Plaintiff 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 Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

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

69. 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.

70. 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.

71. 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.

72. 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.

73. 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]

74. 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

[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).

information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[9]

75. 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.

Plaintiff and Class Members Damages.

76. The ramifications of Defendant's failure to keep Plaintiff's and Class members' PII secure are long lasting and severe. Once that kind of information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[10]

77. The PII belonging to Plaintiff and Class members is private, sensitive in nature, and left inadequately protected by Defendant—who did not obtain Plaintiff's or Class members' consent to disclose such information to any other person as required by applicable law and industry standards.

78. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access,

[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).

[10] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Sept. 9, 2021).

use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

79. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect member data.

80. Defendant could have prevented the intrusions into its systems and, ultimately, the theft of PII if Defendant had remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field.

81. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members are now in imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to dedicate time and resources which they otherwise would have dedicated to other life demands, such as work and family, to mitigate the actual and potential impact of the Data Breach on their lives.

82. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had PII or PHI used for fraudulent purposes, 29% spent a month or more resolving problems," and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[11]

83. In the breach notification letter, Defendant made an offer of 12–months of identity monitoring services to its patients. This is wholly inadequate to compensate Plaintiff and Class members as it fails to provide for the fact victims of data breaches and other unauthorized

[11] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed Sept. 9, 2021).

disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class members' PII.

84. As a direct result of the Defendant's failures to prevent the Data Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;
b. Out–of–pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
c. Lost opportunity costs and lost wages associated with efforts expended and loss of productivity from addressing and attempting to mitigate actual and future consequences of the Data Breach, including but not limited to researching how to prevent, detect, contest, and recover from identity theft and fraud;
d. The present and continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in its possession; and
e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

85. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring their PII is secure, remains secure, and is not subject to further misappropriation and theft.

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

CLASS ACTION ALLEGATIONS

87. Plaintiff brings this suit on behalf of himself and a class and state subclasses of similarly situated individuals which are preliminarily defined as:

> All persons whose PII stored or possessed by SGL was subject to the Data Breach announced by SGL on or about January 21, 2022. (the "Class").
>
> All residents of the State of California whose PII stored or possessed by SGL was subject to the Data Breach announced by SGL on or about January 21, 2022 (the "California Subclass").

88. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; Class Counsel; and all judges assigned to hear any aspect of this litigation, as well as their staff and immediate family members.

89. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

90. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. Defendant has identified more than 10,000 persons whose PII may have been improperly accessed in the Data Breach, and the Class is identifiable within Defendant's records. A precise number of class members can be ascertained through appropriate discovery and from records maintained by Defendant.

91. **Commonality and Predominance:** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class members. These include but are not limited to, the following:

a. Whether Plaintiff's and the Class members' PII was accessed and/or viewed by one or more unauthorized persons in the Data Breach alleged above;
b. Whether Defendant's publishing Plaintiff's and Class members' PII to unauthorized persons was permissible without the prior written authorization of the Plaintiff or the Class members;
c. When and how Defendant should have learned and actually learned of the Data Breach;
d. Whether Defendant's response to the Data Breach was adequate;
e. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;
f. Whether Defendant breached that duty;
g. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class members' PII;
h. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class members' PII;
i. Whether Defendant knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class members' PII secure and prevent loss or misuse of that PII;
j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
k. Whether Defendant caused Plaintiff and Class members damages;
l. Whether Defendant violated the law by failing to promptly notify Plaintiff and

Class members that their PII was compromised;

m. Whether Plaintiff and Class members are entitled to actual damages, nominal and/or statutory damages, credit monitoring, other monetary relief, and/or equitable relief; and

n. Whether Defendant violated the California Unfair Competition Law (Business & Professions Code § 17200, *et seq*.).

92. There are no defenses of a unique nature that may be asserted against the Plaintiff individually, as distinguished from the other members of the class, and the relief sought is common to the class.

93. **Typicality:** Plaintiff's claims are typical of those of other Class members because all had their PII compromised because of the Data Breach, due to Defendant's identical conduct.

94. **Adequacy of Representation:** Plaintiff will fairly and adequately represent and protect the interests of the Class members in that Plaintiff's interests are aligned with the class. Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiff seeks no relief that is adverse to Class members. In addition, Plaintiff retained counsel experienced in data breach and complex consumer class action litigation. Neither Plaintiff nor their counsel have any interests which might cause them not to vigorously pursue this claim.

95. **Superiority:** Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively

modest claims by certain class members, who could not individually afford to litigate a complex claim against large entities, like Defendant. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

96. The prosecution of separate actions by individual members of the class would create a risk of inconsistent or varying adjudications with respect to individual members of the class, and a risk that any adjudications with respect to individual members of the class would, as a practical matter, either be dispositive of the interests of other members of the class not party to the adjudication or substantially impair or impede their ability to protect their interests.

97. Class certification is also warranted for purposes of injunctive and declaratory relief because the defendant has acted, or refused to act, on grounds generally applicable to the class, so that final injunctive and declaratory relief are appropriate with respect to the class as a whole.

CAUSES OF ACTION

FIRST COUNT

Negligence

(On Behalf of Plaintiff, the Class, or alternatively the California Subclass)

98. Plaintiff re-alleges and incorporates by reference the Paragraphs above as if fully set forth herein.

99. Defendant's own negligent conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendant's negligence included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's negligence also included its decision not to comply with (1) industry standards, and/or best practices for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class members; or (2) Section 5 of the FTC Act.

100. First, Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing its security protocols to ensure PII in Defendant's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on relevant cybersecurity measures. Defendant also had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiff's and Class members' PII.

101. As a condition of employment, Plaintiff and Class members were obligated to provide Defendant with their PII. As such, Plaintiff and the Class members entrusted their PII to Defendant with the understanding Defendant would safeguard their information.

102. Defendant was in a position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach. However, Plaintiff and Class members had no ability to protect their PII in Defendant's possession.

103. Defendant had full knowledge of the sensitivity of the PII, and the types of harm Plaintiff and Class members could, would, and will suffer if the information were wrongfully disclosed.

104. Defendant admitted that its computer system containing Plaintiff's and Class members' PII was wrongfully compromised and accessed by unauthorized third persons, and that the Data Breach occurred due to Defendant's actions and/or omissions.

105. Plaintiff and Class members were the foreseeable and probable victims of Defendant's negligent and inadequate security practices and procedures that led to the Data Breach. Defendant knew or should have known of the inherent risks in collecting and storing the highly valuable PII of Plaintiff and Class members, the critical importance of providing adequate

security of that information, the current cyber security risks being perpetrated, and that Defendant had inadequate employee training, monitoring and education and IT security protocols in place to secure the PII of Plaintiff and Class members.

106. Defendant negligently, through its actions and/or omissions, and unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class members' PII while the information was within Defendant's possession and/or control by failing to comply with and/or deviating from standard industry rules, regulations, and practices at the time of the Data Breach.

107. Second, Defendant's violations of Section 5 of the FTC Act constitute negligence. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

108. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class members' PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it required, obtained, and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class members.

109. Plaintiff and Class members are within the class of persons the FTC Act was intended to protect.

110. The harm the Data Breach caused, and continues to cause, is the type of harm the FTC Act was intended to guard against. The FTC pursues 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 Plaintiff and Class members.

111. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of Plaintiff's and Class members' PII.

112. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff and Class members the existence and scope of the Data Breach.

113. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class members, Plaintiff's and Class members' PII would not have been compromised.

114. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and the harm suffered, and/or risk of present and continual harm suffered, by Plaintiff and Class members.

115. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered, and continue to suffer, injuries and damages arising from the Data Breach, including, but not limited to: damages from lost time and efforts to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months—if not years—to discover, detect, and remedy.

116. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered, and will continue to suffer, the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized

disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

Second Cause of Action

Negligence *Per Se*

(On Behalf of Plaintiff and the Class)

117. Plaintiff re-alleges and incorporates by reference the Paragraphs above as if fully set forth herein.

118. 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 Plaintiff's and Class Members' Private Information.

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

120. 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 Plaintiff and the Class.

121. Defendant breached its duties to Plaintiff 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 Plaintiff's and Class Members' Private Information.

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

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

124. The injury and harm suffered by Plaintiff 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 Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

Third Cause of Action

Breach of Implied Contract

(On Behalf of Plaintiff and the Class)

126. Plaintiff incorporates by reference the Paragraphs above as if fully set forth herein.

127. Plaintiff and Class members were required to provide their PII, including their names and Social Security numbers to Defendant as a condition of employment.

128. Plaintiff and Class members providing their PII and their labor to Defendant in exchange for services, along with Defendant's promise to protect their PII from unauthorized disclosure.

129. Upon information and belief, in its written privacy policies, Defendant expressly promised Plaintiff and Class members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

130. Implicit in the agreement between Plaintiff and Class members on the one hand, and the Defendant on the other, regarding providing PII, was Defendant's obligation to: (a) use such PII for business purposes only; (b) take reasonable steps to safeguard that PII; (c) prevent unauthorized disclosures of the PII; (d) provide Plaintiff and Class members with prompt and

sufficient notice of any and all unauthorized access and/or theft of their PII; (e) reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosure or uses; and (f) retain the PII only under conditions that kept such information secure and confidential.

131. Without such implied contracts, Plaintiff and Class members would not have provided their PII to Defendant.

132. Plaintiff and Class members fully performed their obligations under the implied contract with Defendant. However, Defendant did not.

133. Defendant breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' PII, which was compromised as a result of the Data Breach.

134. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class members have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months if not years to discover, detect, and remedy.

Fourth Cause of Action

Breach of Confidence

(On Behalf of Plaintiff and the Class)

135. Plaintiff incorporates by reference the Paragraphs above as if fully set forth herein.

136. At all times during Plaintiff's and Class members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class members' PII that Plaintiff and Class members provided to Defendant.

137. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

138. Plaintiff and Class members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the information to be disseminated to any unauthorized parties.

139. Plaintiff and Class members also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of protecting its networks and data systems.

140. Defendant required and voluntarily received, in confidence, Plaintiff's and Class members' PII with the understanding that the information would not be disclosed or disseminated to the public or any unauthorized third parties.

141. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class members' PII, Plaintiff's and Class members' PII was disclosed to, and misappropriated by, unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

142. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class members have suffered, and will continue to suffer damages.

143. But for Defendant's disclosure of Plaintiff's and Class members' PII in violation of the parties' understanding of confidence, Plaintiff's and Class members' PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class members' PII, as well as the resulting damages.

144. The injury and harm Plaintiff and Class members suffered, and continue to suffer, was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class members' PII. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class members' PII had numerous security and other vulnerabilities placing Plaintiff's and Class members' PII in jeopardy.

145. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) 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; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the

remainder of the lives of Plaintiff and Class members; and (g) the diminished value of Defendant's services they received.

146. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non–economic losses.

Fifth Cause of Action

Violation of the California Unfair Competition Law,

Cal. Bus. & Prof. Code § 17200, *et seq*.--Unfair Business Practices

(On Behalf of Plaintiff and the California Subclass)

147. Plaintiff incorporates by reference the Paragraphs above as if fully set forth herein.

148. Defendant violated Cal. Bus. & Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair, or fraudulent business acts and practices, and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code § 17200 with respect to the services provided to Plaintiff and California Subclass members.

149. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub–standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and California Subclass members' PII with knowledge the information would not be adequately protected; and by storing Plaintiff's and California Subclass members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which require Defendant to take reasonable methods of safeguarding the PII of Plaintiff and California Subclass members.

150. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

151. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and California Subclass members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Plaintiff's and California Subclass members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described herein.

152. Defendant knew or should have known Defendant's computer systems and data security practices were inadequate to safeguard Plaintiff's and California Subclass members' PII and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above–named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the California Subclass members.

153. Plaintiff, on behalf of the California Subclass, seeks relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Class members of money or property Defendant may have acquired by means of Defendant's unlawful, and unfair business practices, restitutionary disgorgement of all monies that accrued to Defendant because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

Sixth Cause of Action
Violation of the California Consumer Privacy Act,
Cal. Civ. Code §§ 1798.100, *et seq*.
(On Behalf of Plaintiff and the California Subclass)

154. Plaintiff incorporates by reference Paragraphs 1 through 96 above as if fully set forth herein.

155. Defendant violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff and California Subclass Members' nonencrypted and

nonredacted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and California Subclass Members.

156. As a direct and proximate result of Defendant's acts, Plaintiff's and the California Subclass Members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendant's computer systems and/or from the dark web, where hackers further disclosed Defendant's customers' PII.

157. As a direct and proximate result of Defendant's acts, Plaintiff and the California Subclass Members were injured and lost money or property, including but not limited to, the loss of California Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

158. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard California Subclass Members' PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass Members.

159. Defendant collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

160. At this time, Plaintiff and California Subclass Members seek only actual pecuniary damages suffered as a result of Defendant's violations of the CCPA, injunctive and declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and any other relief the court deems proper.

161. On February 3, 2022, Plaintiff mailed Defendant notice in writing, via U.S. certified mail, which identified the specific provisions of this title he alleges Navistar has violated. If within 30 days of Plaintiff's written notice Defendant fails to "actually cure" its violation of Cal. Civ. Code § 1798.150(a) and provide "an express written statement that the violations have been cured and that no further violations shall occur," Plaintiff will amend this complaint to also seek the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and all Class members, request judgment against the Defendant, and that the Court grant the following:

A. An order certifying the Class as defined herein, and appointing Plaintiff and their Counsel to represent the Class;

B. Granting injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members, including but not limited to an order:

i. prohibiting SGL from engaging in the wrongful and unlawful acts described herein,

ii. requiring SGL to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws,

iii. requiring SGL to delete, destroy, and purge the PII of Plaintiff and Class members unless SGL can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class members,

iv. requiring SGL to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class members,

v. prohibiting SGL from maintaining Plaintiff's and Class members' PII on a cloud-based database,

vi. requiring SGL to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on SGL's systems on a periodic basis, and ordering SGL to promptly correct any problems or issues detected by such third-party security auditors,

vii. requiring SGL to engage independent third-party security auditors and internal personnel to run automated security monitoring,

viii. requiring SGL to audit, test, and train its security personnel regarding any new or modified procedures,

ix. requiring SGL to conduct regular database scanning and securing checks,

x. requiring SGL to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class members,

xi. requiring SGL to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,

xii. requiring SGL to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees'

compliance with SGL's policies, programs, and systems for protecting PII,

xiii. requiring SGL to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor SGL's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated,

xiv. requiring SGL to meaningfully educate all Class members about the threats that they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves,

xv. requiring SGL to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected,

xvi. requiring SGL disclose any future data disclosures in a timely and accurate manner; and

xvii. requiring SGL to provide ongoing credit monitoring and identity theft repair services to Class members.

C. An award of compensatory, statutory, and nominal damages in an amount to be determined;

D. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

F. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury.

Dated: February 9, 2022

Respectfully submitted,

/s/ *Roopal P. Luhana*
CHAFFIN LUHANA LLP
Roopal P. Luhana, Esq.
Steven Cohn, Esq. (*pro hac vice forthcoming*)
600 Third Avenue, 12th Floor
New York, NY 10016
Phone: 888-480-1136
Fax: 888-499-1123
luhana@chaffinluhana.com
cohn@chaffinluhana.com

MASON LIETZ & KLINGER LLP
Gary M. Klinger (*pro hac vice* forthcoming)
221 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: (202) 975-0477
gklinger@masonllp.com

Attorneys for Plaintiff and the Proposed Class

CERTIFICATION PURSUANT TO R. 4:5-1

Plaintiff, by his attorneys, hereby certifies that the matter in controversy is not the subject of any other pending or contemplated judicial or arbitration proceedings. Plaintiff is not currently aware of any other parties that should be joined in this particular action. In addition, Plaintiff recognizes his continuing obligation to file and serve on all parties and the Court an amended certification if there is a change in the facts stated in this original certification.

Dated: February 9, 2022

Respectfully submitted,

/s/ *Roopal P. Luhana*
CHAFFIN LUHANA LLP
Roopal P. Luhana, Esq.
Steven Cohn, Esq. (*pro hac vice forthcoming*)
600 Third Avenue, 12th Floor
New York, NY 10016
Phone: 888-480-1136
Fax: 888-499-1123
luhana@chaffinluhana.com
cohn@chaffinluhana.com

MASON LIETZ & KLINGER LLP
Gary M. Klinger (*pro hac vice* forthcoming)
221 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: (202) 975-0477
gklinger@masonllp.com

Attorneys for Plaintiff and the Proposed Class

Civil Case Information Statement
(CIS)

Use for initial Law Division
Civil Part pleadings (not motions) under *Rule* 4:5-1
Pleading will be rejected for filing, under *Rule* 1:5-6(c), if information above the black bar is not completed or attorney's signature is not affixed

For Use by Clerk's Office Only
Payment type: ☐ ck ☐ cg ☐ ca
Chg/Ck Number:
Amount:
Overpayment:
Batch Number:

Attorney/Pro Se Name	Telephone Number	County of Venue
Roopal P. Luhana, Esq.	(347) 269-4461	Atlantic

Firm Name (if applicable)	Docket Number (when available)
Chaffin Luhana LLP	

Office Address	Document Type
600 Third Avenue, 12th Floor New York, NY 10016	Class Action Complaint
	Jury Demand ■ Yes ☐ No

Name of Party (e.g., John Doe, Plaintiff)	Caption
EDWARD GONSHOROWSKI, on behalf of himself and all others similarly situated	EDWARD GONSHOROWSKI, on behalf of himself and all others similarly situated v. SPENCER GIFTS LLC

Case Type Number (See reverse side for listing)	Are sexual abuse claims alleged?	Is this a professional malpractice case?
699	☐ Yes ■ No	☐ Yes ■ No If you have checked "Yes," see *N.J.S.A.* 2A:53A-27 and applicable case law regarding your obligation to file an affidavit of merit.

Related Cases Pending?	If "Yes," list docket numbers
☐ Yes ■ No	

Do you anticipate adding any parties (arising out of same transaction or occurrence)?	Name of defendant's primary insurance company (if known)
☐ Yes ■ No	☐ None ■ Unknown

The Information Provided on This Form Cannot be Introduced into Evidence.

Case Characteristics for Purposes of Determining if Case is Appropriate for Mediation

Do parties have a current, past or recurrent relationship?	If "Yes," is that relationship:
☐ Yes ■ No	☐ Employer/Employee ☐ Friend/Neighbor ☐ Other (explain) ☐ Familial ☐ Business

Does the statute governing this case provide for payment of fees by the losing party? ☐ Yes ■ No

Use this space to alert the court to any special case characteristics that may warrant individual management or accelerated disposition
Proposed Class Action

Do you or your client need any disability accommodations?	If yes, please identify the requested accommodation:
☐ Yes ■ No	
Will an interpreter be needed?	If yes, for what language?
☐ Yes ■ No	

I certify that confidential personal identifiers have been redacted from documents now submitted to the court and will be redacted from all documents submitted in the future in accordance with *Rule* 1:38-7(b).

Attorney Signature: */s/ Roopal Luhana*

Side 2

Civil Case Information Statement
(CIS)

Use for initial pleadings (not motions) under *Rule* 4:5-1

CASE TYPES (Choose one and enter number of case type in appropriate space on the reverse side.)

Track I - 150 days discovery

151	Name Change
175	Forfeiture
302	Tenancy
399	Real Property (other than Tenancy, Contract, Condemnation, Complex Commercial or Construction)
502	Book Account (debt collection matters only)
505	Other Insurance Claim (including declaratory judgment actions)
506	PIP Coverage
510	UM or UIM Claim (coverage issues only)
511	Action on Negotiable Instrument
512	Lemon Law
801	Summary Action
802	Open Public Records Act (summary action)
999	Other (briefly describe nature of action)

Track II - 300 days discovery

305	Construction
509	Employment (other than Conscientious Employees Protection Act (CEPA) or Law Against Discrimination (LAD))
599	Contract/Commercial Transaction
603N	Auto Negligence – Personal Injury (non-verbal threshold)
603Y	Auto Negligence – Personal Injury (verbal threshold)
605	Personal Injury
610	Auto Negligence – Property Damage
621	UM or UIM Claim (includes bodily injury)
699	Tort – Other

Track III - 450 days discovery

005	Civil Rights
301	Condemnation
602	Assault and Battery
604	Medical Malpractice
606	Product Liability
607	Professional Malpractice
608	Toxic Tort
609	Defamation
616	Whistleblower / Conscientious Employee Protection Act (CEPA) Cases
617	Inverse Condemnation
618	Law Against Discrimination (LAD) Cases

Track IV - Active Case Management by Individual Judge / 450 days discovery

156	Environmental/Environmental Coverage Litigation
303	Mt. Laurel
508	Complex Commercial
513	Complex Construction
514	Insurance Fraud
620	False Claims Act
701	Actions in Lieu of Prerogative Writs

Multicounty Litigation (Track IV)

271	Accutane/Isotretinoin
274	Risperdal/Seroquel/Zyprexa
281	Bristol-Myers Squibb Environmental
282	Fosamax
285	Stryker Trident Hip Implants
286	Levaquin
289	Reglan
291	Pelvic Mesh/Gynecare
292	Pelvic Mesh/Bard
293	DePuy ASR Hip Implant Litigation
295	AlloDerm Regenerative Tissue Matrix
296	Stryker Rejuvenate/ABG II Modular Hip Stem Components
297	Mirena Contraceptive Device
299	Olmesartan Medoxomil Medications/Benicar
300	Talc-Based Body Powders
601	Asbestos
623	Propecia
624	Stryker LFIT CoCr V40 Femoral Heads
625	Firefighter Hearing Loss Litigation
626	Abilify
627	Physiomesh Flexible Composite Mesh
628	Taxotere/Docetaxel
629	Zostavax
630	Proceed Mesh/Patch
631	Proton-Pump Inhibitors
632	HealthPlus Surgery Center
633	Prolene Hernia System Mesh
634	Allergan Biocell Textured Breast Implants

If you believe this case requires a track other than that provided above, please indicate the reason on Side 1, in the space under "Case Characteristics.

Please check off each applicable category ■ **Putative Class Action** ☐ **Title 59** ☐ **Consumer Fraud**

Civil Case Information Statement

Case Details: ATLANTIC | Civil Part Docket# L-000311-22

Case Caption: GONSHOROWSKI EDWARD VS SPENCER GIFTS LLC
Case Initiation Date: 02/09/2022
Attorney Name: ROOPAL P LUHANA
Firm Name: CHAFFIN LUHANA LLP
Address: 600 THIRD AVE 12TH FL
NEW YORK NY 10016
Phone: 3472694472
Name of Party: PLAINTIFF : GONSHOROWSKI, EDWARD
Name of Defendant's Primary Insurance Company (if known): Unknown

Case Type: TORT-OTHER
Document Type: Complaint with Jury Demand
Jury Demand: YES - 12 JURORS
Is this a professional malpractice case? NO
Related cases pending: NO
If yes, list docket numbers:
Do you anticipate adding any parties (arising out of same transaction or occurrence)? NO

Are sexual abuse claims alleged by: EDWARD GONSHOROWSKI? NO

THE INFORMATION PROVIDED ON THIS FORM CANNOT BE INTRODUCED INTO EVIDENCE

CASE CHARACTERISTICS FOR PURPOSES OF DETERMINING IF CASE IS APPROPRIATE FOR MEDIATION

Do parties have a current, past, or recurrent relationship? NO

If yes, is that relationship:

Does the statute governing this case provide for payment of fees by the losing party? NO

Use this space to alert the court to any special case characteristics that may warrant individual management or accelerated disposition:
Proposed Class Action

Do you or your client need any disability accommodations? NO
If yes, please identify the requested accommodation:

Will an interpreter be needed? NO
If yes, for what language:

Please check off each applicable category: Putative Class Action? YES **Title 59?** NO **Consumer Fraud?** YES

I certify that confidential personal identifiers have been redacted from documents now submitted to the court, and will be redacted from all documents submitted in the future in accordance with *Rule* 1:38-7(b)

02/09/2022
Dated

/s/ ROOPAL P LUHANA
Signed