**UNITED STATES DISTRICT COURT**
**FOR THE SOUTHERN DISTRICT OF NEW YORK**

| | |
|---|---|
| JAE LEE, on behalf of himself and all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>TARO PHARMACEUTICALS U.S.A., INC.,<br><br>Defendant. | Case No. 7:23-cv-03834-CS<br><br>**AMENDED CLASS ACTION COMPLAINT**<br><br>DEMAND FOR JURY TRIAL |

Jae Lee, ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Taro Pharmaceuticals U.S.A. Inc., ("Taro" or "Defendant") and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel's investigations, and facts of public record.[1]

## INTRODUCTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant Taro is an international pharmaceutical company that claims to develop high-quality, proprietary, and off-patent pharmaceuticals for markets in the United States, Canada, Israel, and other countries around the world.

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") about its current and former employees. But Defendant lost control over that

[1] Attached as Exhibits A and B are copies of Taro's official data breach notices.

data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. Thus, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to employee PII.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII. In short, Defendant's failures placed the Class's PII in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim, receiving breach notice on or about April 20, 2023. He brings this class action on behalf of himself, and all others harmed by Defendant's misconduct.

## PARTIES

7. Plaintiff, Jae Lee, is a natural person and citizen of New York. He resides in White Plains, New York where he intends to remain.

8. Defendant, Taro, is a domestic business corporation with its principal place of business at 3 Skyline Drive, Hawthorne, New York 10532.

## JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are over 100 putative Class Members, and Class members are citizens of different state than Defendant.

10. This Court has personal jurisdiction over Defendant because it is headquartered in New York, regularly conducts business in New York, and has sufficient minimum contacts in New York.

11. Venue is proper in this Court under because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

## BACKGROUND

***Defendant Collected and Stored the PII of Plaintiff and the Class***

12. Defendant is an international pharmaceutical company with its United States' headquarters in Hawthorne, New York.[2]

13. As part of its business, Defendant receives and maintains the PII of thousands of current and former employees. In doing so, Defendant implicitly promises to safeguard their PII.

14. In collecting and maintaining the PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

15. Under state and federal law, businesses like Defendant have duties to protect employees' PII and to notify them about breaches.

16. Defendant recognizes these duties, declaring that:

a. "We are committed to maintaining the confidentiality of your personal information."[3]

[2] *Contact*, TARO, https://taro.com/contact (last accessed May 4, 2023).
[3] *Privacy Statement*, TARO, https://taro.com/privacy-statement (last accessed May 4, 2023).

b. "We do not sell your personal information and we do not disclose such information except as permitted or required by law."[4]

c. "Whether you are a patient, healthcare provider, investor, customer or job applicant, respect for the privacy of your personal information is very important to us."[5]

d. "Taro [is] committed to collecting, maintaining and securing your personal information in strict accordance with the terms of this policy."[6]

e. "Personal data available to Taro . . . is processed only in accordance with the guidelines established in the Privacy Statement."[7]

17. Furthermore, in its official "Code of Conduct" publication, Taro declares that it: "is committed to protecting [private] information responsibly, in accordance with relevant privacy laws."[8] Taro specifically declares that such private information includes:

a. "Government-issued identification numbers;"

b. "Contact information;"

c. "Employment history, including reviews and salary information;"

d. "Marital status and information about [] families;"

e. "Medical history, which may include disability claims."[9]

18. Similarly, in its official "Code of Ethics for the CEO and Senior Officers," Taro declares that it must:

---

[4] *Id*.
[5] *Id*.
[6] *Id*.
[7] *Terms of Use*, TARO, https://taro.com/terms-of-use (last accessed Sept. 27, 2023).
[8] *Code of Conduct*, TARO (2014) https://www.taro.com/media/oMedia/TaroCOC.pdf.
[9] *Id*.

a. "Protect the confidentiality of non-public information . . . and prevent the unauthorized disclosure of such information."[10]

19. And again, in its Data Breach notices, Defendant declares that:

a. "Taro Pharmaceuticals U.S.A., Inc. ("Taro") takes the privacy and security of personal information very seriously."[11]

b. "Taro remains dedicated to protecting the personal information in its control."[12]

***Defendant's Data Breach***

20. On March 3, 2023, Defendant was hacked in a Data Breach. It is unclear how long that Data Breach lasted, but it was not discovered until March 25, 2023, giving criminals plenty of time to seize Plaintiff's and the Class's exposed PII. Moreover, Defendant did not provide victims with notice of the Data Breach until April 19, 2023.[13]

21. Simply put, Defendant failed in its duties when its inadequate security practices caused the Data Breach.

22. Because of Defendant's Data Breach, at least the following types of PII were compromised in a targeted cyberattack aimed at obtaining this exact kind of valuable PII:

a. names;

b. Social Security numbers;

c. state identification numbers;

d. passport numbers; and

---

[10] *Code of Ethics*, TARO, https://www.taro.com/media/oMedia/Code-of-Ethics.pdf (last accessed Sept. 27, 2023).
[11] Ex. A, at 1.
[12] Ex. B, at 2.
[13] *Data Breach Notifications*, OFFICE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/0cdf5581-aaa2-4bd6-90da-a32de4114a97.shtml (last accessed May 4, 2023).

e. driver's license numbers.[14]

23. This Data Breach was not merely a hiccup or glitch in Defendant's data systems. Rather, this Data Breach was caused by the intentional (and successful) targeting of highly sensitive information by sophisticated cybercriminals. After all, Defendant itself dubbed the hackers as "the perpetrators."[15]

24. Defendant admitted that the Data Breach included (1) the "breach of certain file systems" and (2) "the *theft* of certain company data and personal data."[16]

25. The actual "theft of certain company data and personal data" from a large corporation like Taro does not occur by accident. Rather, Taro's admission—of the *actual theft* of personal data—underscores the seriousness of the Data Breach and speaks to the severity of the injuries suffered by Plaintiff and the Class.

26. And again—although in more euphemistic language—Defendant confirmed that "an unknown actor gained access to and obtained some data from our network."[17]

27. Defendant further confirmed the severity of the Data Breach (and its resulting injuries) by declaring that it "took steps to contain and remediate its impact, including employing containment protocols to mitigate the threat."[18] This language reveals the danger caused by the Data Breach. After all, a benign or accidental data incident would not require "contain[ing]," "remediat[ing]," or "mitigate[ing]."[19]

[14] Ex. B, at 1.
[15] *Id*. at 2.
[16] *Id.* at 1 (emphasis added).
[17] Ex. A, at 1.
[18] Ex. B, at 1.
[19] *See id*.

28. But, like a toxic waste spill, this Data Breach was severe—and thus necessitated urgent steps "to contain and remediate" and "to mitigate the threat."[20]

29. In total, Defendant injured at least 1,734 persons—via the exposure of their PII—in the Data Breach.[21] Upon information and belief, these persons include Defendant's current and former employees.

30. And yet, Defendant waited weeks before it began notifying the Class.[22]

31. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

32. And when it did notify Plaintiff and the Class of the Data Breach, Defendant downplayed the seriousness of the risk stating, "we have no evidence that anyone's data has been misused" but that "we recommend that you remain vigilant by reviewing your account statements and credit reports closely."[23]

33. However, despite downplaying the risk, Defendant warned breach victims to take steps "to protect your information."[24]

34. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

35. Defendant's negligence is further revealed by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. In fact, Defendant's cybersecurity was so deficient

---

[20] *Id*.
[21] *Data Breach Notifications*, OFFICE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/0cdf5581-aaa2-4bd6-90da-a32de4114a97.shtml (last accessed May 4, 2023).
[22] *Id*.
[23] Ex. A, at 1, 3.
[24] *Id.* at 2.

that it did not even detect that the breach was occurring until three full weeks after it began, giving the cybercriminals unfettered access to Plaintiff's and the Class's PII during that time.

36. The severity of Defendant's negligence is further evidenced by the sweeping security changes that Defendant implemented—but only after the Data Breach already injured Plaintiff and the Class. Specifically, Defendant claims to have:

a. "implemented additional security features to protect the network;"

b. "employ[ed] containment protocols to mitigate the threat;"

c. "[employed] additional measures to ensure the integrity of our IT systems' infrastructure and data;"

d. "ret[ained] cyber security experts;" and

e. "use[d] enhanced security measures to address and mitigate the impact of the incident."[25]

37. But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary to safeguard the PII it collects and stores—should have been implemented *before* the Data Breach.

38. Defendant has done little to remedy its Data Breach. True, Defendant has offered concessions of credit monitoring to Plaintiff and the Class.[26] But upon information and belief, such services do not properly compensate Plaintiff and Class Members for the injuries that Defendant inflicted upon them.

[25] *Id*. at 1.
[26] *Id*.

39. Because of Defendant's Data Breach, the sensitive PII of the Plaintiff and Class Members were placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

***Plaintiff Lee's Experiences and Injuries***

40. Plaintiff Jae Lee was injured by Defendant's Data Breach.

41. He was employed by Defendant for five years, but his employment ended years ago in 2019.

42. As a condition of his employment with Defendant, Plaintiff provided Defendant with his PII. Defendant used that PII to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

43. Plaintiff provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

44. Plaintiff does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

45. Through its Data Breach, Defendant compromised Plaintiff's PII. To which, Plaintiff received a Notice of Data Breach dated April 19, 2023.

46. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft, and, in fact, Defendant directed him to take those steps in its breach notice. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

47. For example, on April 27, 2023, Plaintiff Lee spent time trying to call the phone number provided by Defendant to learn more about his exposure. But Defendant did not answer Plaintiff Lee's call. And since then, Plaintiff Lee waited—and is still waiting—to hear back from Defendant.

48. Since being notified of the Data Breach, Plaintiff Lee spent at least fifteen (15) hours carefully monitoring his various financial accounts for signs of identity theft and fraud. In addition, Plaintiff Lee spent at least four (4) hours attempting to contact Defendant to learn more about the Data Breach and the extent of his exposure.

49. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

50. Plaintiff suffered actual injury from the exposure (and likely theft) of his PII—which violates his rights to privacy.

51. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

52. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

53. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

54. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

***Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft***

55. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII is used;

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII; and

h. continued risk to their PII—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

56. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

57. The value of Plaintiff's and Class's PII on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

58. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

59. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

60. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

61. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

62. Defendant disclosed the PII of Plaintiff and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

63. Defendant's failure to promptly and properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

***Defendant Knew—Or Should Have Known—of the Risk of a Data Breach***

64. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in recent years.

65. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[27]

66. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[28]

---

[27] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

[28] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

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

***Defendant Failed to Follow FTC Guidelines***

68. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

69. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[29] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

70. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

71. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

[29] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

72. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use 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.

73. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to current and former employees' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

***Defendant Failed to Follow Industry Standards***

74. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: 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.

75. Other industry standard best practices 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.

76. 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.

77. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

## CLASS ACTION ALLEGATIONS

78. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach discovered by Taro in March 2023, including all those who received notice of the Data Breach.

79. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

80. Plaintiff reserves the right to amend the class definition.

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

82. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

83. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable.

84. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

b. if 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. if Defendant were negligent in maintaining, protecting, and securing PII;

d. if Defendant breached implied contractual promises to safeguard Plaintiff's and the Class's PII;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff's and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

85. Typicality. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

86. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class members' interests. And the Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

87. Superiority. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

## FIRST CAUSE OF ACTION
**Negligence**
**(On Behalf of Plaintiff and the Class)**

88. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

89. Plaintiff and Class Members entrusted their PII to Defendant.

90. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

91. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

92. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

93. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff's and Class Members' PII.

94. Defendant owed—to Plaintiff and Class Members—at least the following duties:

a. to exercise reasonable care in handling and using the PII in its care and custody;

b. to implementing industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. to promptly detect attempts at unauthorized access; and

d. to notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII.

95. Also, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

96. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain pursuant to regulations.

97. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

98. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because the Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining employment from Defendant.

99. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

100. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff's and Class Members' and the importance of exercising reasonable care in handling it.

101. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

102. Defendant breached these duties as evidenced by the Data Breach.

103. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII by:

a. disclosing and providing access to this information to third parties; and

b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

104. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff's and Class Members' injury.

105. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact.

106. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

107. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

108. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

109. 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 its current and former employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive PII.

110. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect 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 Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

111. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because 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 members of the Class.

112. Defendant had a duty to Plaintiff and Class Members to implement and maintain reasonable security procedures and practices to safeguard PII.

113. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

114. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

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

116. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII and PHI.

117. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

## SECOND CAUSE OF ACTION
**Breach of Implied Contract**
**(On Behalf of Plaintiff and the Class)**

118. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

119. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving employment from Defendant. Plaintiff and Class Members provided their PII to Defendant or its third-party agents in exchange for employment with Defendant.

120. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant in exchange for employment.

121. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

122. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

123. Plaintiff and the Class reasonably believed that, in exchange for their employment services, Defendant would provide adequate security protections for the PII that they were required to provide to Defendant.

124. After all, Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

125. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

126. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

127. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

128. Defendant materially breached the contracts it entered with Plaintiff and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

129. In these and other ways, Defendant violated its duty of good faith and fair dealing.

130. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed *supra*).

131. Plaintiff and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

**THIRD CAUSE OF ACTION**
**Unjust Enrichment**
**(On Behalf of Plaintiff and the Class)**

132. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

133. This claim is pleaded in the alternative to the breach of implied contract claim.

134. Plaintiff and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to facilitate its provision of employment.

135. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members. And Defendant benefited from receiving Plaintiff's and Class Members' PII, as this was used to facilitate its provision of employment.

136. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

137. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

138. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class Members' employment and/or payment because Defendant failed to adequately protect their PII.

139. Plaintiff and Class Members have no adequate remedy at law.

140. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

## FOURTH CAUSE OF ACTION
**Declaratory Judgment**
**(On Behalf of Plaintiff and the Class)**

141. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

142. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

143. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff

allege that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

144. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class Members.

145. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

146. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

147. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff's and Class Members' injuries.

148. If an injunction is not issued, the resulting hardship to Plaintiff and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

149. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

**PRAYER FOR RELIEF**

Plaintiff and Class Members respectfully requests judgment against Defendant and that the Court enter an order:

a. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

b. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

c. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

d. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

e. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

f. Awarding attorneys' fees and costs, as allowed by law;

g. Awarding prejudgment and post-judgment interest, as provided by law;

h. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

i. Granting other relief that this Court finds appropriate.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a jury trial for all claims so triable.

Dated: September 28, 2023

Respectfully submitted,

By: */s/ Raina C. Borrelli*

Raina Borrelli (*pro hac vice*)
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703-3515
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com

James J. Bilsborrow (SB8204)
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
Telephone: (212) 558-5500
jbilsborrow@weitzlux.com

*Attorneys for Plaintiff and Proposed Class*