IN THE CIRCUIT COURT OF THE NINTH JUDICIAL CIRCUIT
IN AND FOR ORANGE COUNTY, FLORIDA

GREGORY PULL, on behalf of himself and all others similarly situated, Plaintiff, v. BAER'S FURNITURE CO., INC. Defendant.	NO. PROPOSED CLASS ACTION DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Gregory Pull ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Baer's Furniture Co., Inc. ("Baer's Furniture" 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.

NATURE OF ACTION

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

2. Defendant is a "premiere home furnishings destination" with locations across the state of Florida.[1]

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] *About*, BAER'S FURNITURE, https://www.baers.com/about/ (last visited July 21, 2023).

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

4. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to current and former 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, having received a breach notice. He brings this class action on behalf of himself, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this data breach, the Class's private information was exactly that—private. Not anymore. Now, the Class's private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Gregory Pull, is a natural person and citizen of Florida. He resides in Orlando, Florida where he intends to remain.

9. Defendant, Baer's Furniture Co., Inc., is a Florida Profit Corporation with its principal place of business at 1589 Northwest 12th Avenue, Pompano Beach, FL 33069.

JURISDICTION AND VENUE

10. The Court has subject matter jurisdiction over Plaintiff's claims under Florida Stat.§ 26.012 and § 86.011. This Court has jurisdiction over this dispute because this complaint seeks damages over $50,000.00, exclusive of interest and attorneys' fees.

11. The Court has personal jurisdiction over Defendant because under Florida Stat. § 48.193, Defendant personally or through its agents operated, conducted, engaged in, or carried on a business or business venture in Florida; had offices in Florida; committed tortious acts in Florida; and because Defendant engaged in significant business activity within Florida.

12. Venue is proper in Broward County under Florida Stat. § 47.011 and § 47.051 because Defendant is headquartered and does business in this county, the causes of action accrued in this county, and Defendant has an office for the transaction of its customary business in this county.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and the Class

13. Defendant is Pompano Beach based home furnishings stores with sixteen locations across Florida.[2] As such, Defendant collects highly sensitive PII of its current and former employees.

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.

[2] *Store*s, BAER'S FURNITURE, https://www.baers.com/stores/ (last visited July 21, 2023).

15. Indeed, Defendant promises in its privacy policy that it implements "reasonable safeguards to help ensure that information [it] collect[s] on the website is secure":

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

Defendant's Data Breach

17. On August 21, 2022, Defendant realized that it had been attacked resulting in its systems being encrypted and the attacker gaining access to Defendant's data.[3]

18. Defendant's Data Breach, at least the following types of PII were compromised:

a. Full names,

b. Addresses;

c. Social Security numbers; and

d. "Potentially medical information."[4]

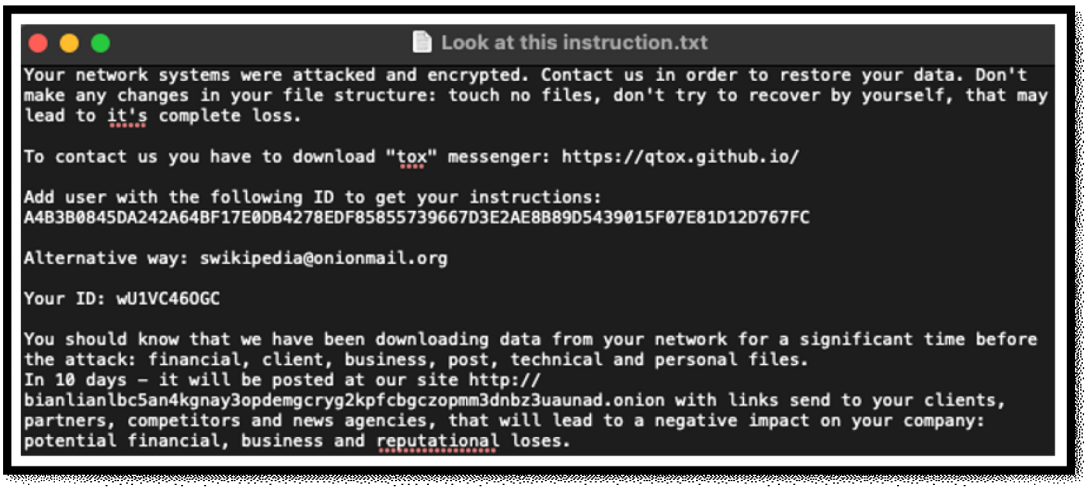
19. On information and belief, the notorious BianLian ransomware took credit for the Data Breach.[5] An incredibly active and successful hacker with over 118 victims[6], BianLian ransomware was known to employ double extortion model by encryption victims' systems after

[3] *Breach Notice,* Attached hereto as Exhibit A.
[4] *Id.*
[5] Breach Sense, https://www.breachsense.io/breaches/baers/ (last visited July 24, 2023).
[6] Bill Toulas, BianLian ransomware gang shifts focus to pure data extortion, https://www.bleepingcomputer.com/news/security/bianlian-ransomware-gang-shifts-focus-to-pure-data-extortion/ (last visited July 24, 2023).

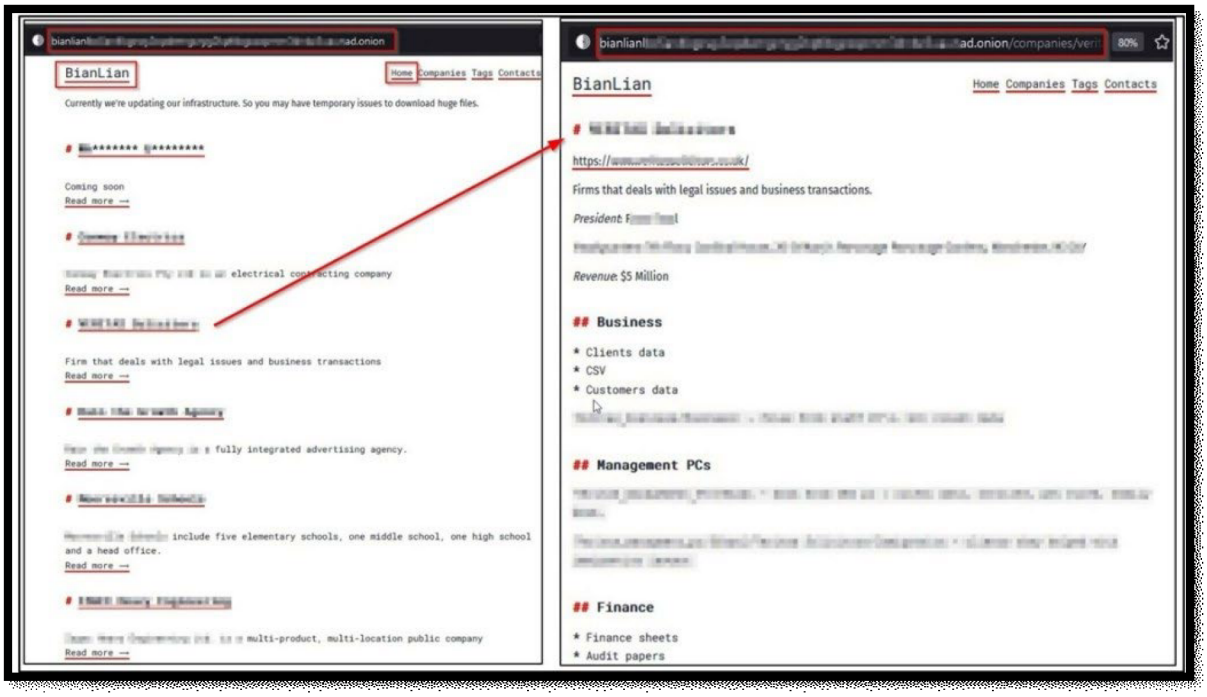
exfiltrating the data.[7] However, BianLian recently announced to have shifted its focus from encrypting its victims' files to exfiltrating data found on compromised or weak networks and using them for extortion.[8] Defendant knew or should have known of the tactics that hackers like BianLian employ.

20. With the PII secured and stolen by BianLian ransomware, the hackers then purportedly issued a ransom demand to Defendant. However, Baer's Furniture has provided no public information on the ransom demand or payment.

21. Following the deadline of a ransom demand, BianLian ransomware is known to release all stolen information obtained from a data breach onto a leak page.[9] An example of the leak page displaying BianLian's standard extortion language and leak site homepage is displayed below[10]:



[7] America's Cyber Defense Agency, Cybersecurity & Infrastructure Security Agency https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a (last visited July 24, 2023).
[8] Bill Toulas, BianLian ransomware gang shifts focus to pure data extortion, https://www.bleepingcomputer.com/news/security/bianlian-ransomware-gang-shifts-focus-to-pure-data-extortion/ (last visited July 24, 2023).
[9] America's Cyber Defense Agency, Cybersecurity & Infrastructure Security Agency https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-136a (last visited July 24, 2023).
[10] BianLian: New Ransomware variant on the rise, https://blog.cyble.com/2022/08/18/bianlian-new-ransomware-variant-on-the-rise/ (last visited July 24, 2023); *see also* https://blogs.blackberry.com/en/2022/10/bianlian-ransomware-encrypts-files-in-the-blink-of-an-eye (last visited July 24, 2023).



22. Defendant has not disclosed the full scope of the Data Breach. But upon information and belief, Defendant's Data Breach injured thousands of individuals via the exposure of their PII. And upon information and belief, these individuals include Defendant's current and former employees.

23. And yet, Defendant waited until March 7, 2023—a full *eighty-four days* after it discovered the breach—before Defendant began notifying the class.

24. 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.

25. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class to "remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports."[11]

[11] *Id.*

26. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages.

27. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

28. Since the breach, Defendant claims to be "securing our systems to protect your information."[12] But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

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

30. Further, the Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

31. Defendant has done little to remedy its Data Breach. True, Defendant has offered credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class members for the injuries that Defendant inflicted upon them.

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

---

[12] *Id.*

Plaintiff's Experiences and Injuries

33. Plaintiff Gregory Pull was employed by Defendant from November 2020 until December 2023.

34. 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 his PII to obtain employment and payment for that employment.

35. As a result, Plaintiff was injured by Defendant's Data Breach.

36. 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.

37. Plaintiff received a Notice of Data Breach on approximately March 13, 2023.

38. Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web. Plaintiff has received numerous notifications from his bank that his information has been found on the dark web.

39. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts and putting a lock on his credit to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

40. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

41. 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.

42. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

43. 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.

44. 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.

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

46. 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

47. 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.

48. 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.

49. The value of Plaintiff 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.

50. 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.

51. 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.).

52. 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.

53. 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 and other Class members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

54. 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.

55. Defendant's failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff 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

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

57. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[13] Of the 1,862 recorded data breaches,

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

330 of them, or 17.7% were in the medical or healthcare industry.[14] Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[15]

58. 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."[16]

59. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[17]

60. 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

61. 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.

---

[14] *Id.*
[15] *Id.*
[16] 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.
[17] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited July 31, 2022).

62. 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.[18] 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.

63. 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.

64. 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;

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.

65. 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

[18] *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.

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

66. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to clients' 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

67. 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.

68. 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.

69. 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.

70. 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

71. Plaintiff brings this class action under the Florida Rules of Civil Procedure 1.220(a) and (b)(3) individually and on behalf of all members of the following class:

> All individuals residing in Florida whose PII was compromised in the Data Breach discovered by Baer's Furniture Co., Inc. in August 2022, including all those who received notice of the breach.

72. 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.

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

74. 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.

75. 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.

76. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least thousands of members. The precise size of the Class can be determined from information in Defendant's possession and control.

77. Typicality. Plaintiff's claims are typical of Class members' 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.

78. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. his interests do not conflict with Class members' interests. And 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.

79. 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 contract promises to safeguard Plaintiff 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 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.

80. 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)

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

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

83. 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.

84. Such a duty is codified in Florida law (*see e.g.,* Fla. Stat. §§ 456.057, 501.171).

85. 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 their PII was wrongfully disclosed.

86. 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 and Class members' PII.

87. Defendant owed—to Plaintiff and Class members—at least the following duties to:

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

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

c. promptly detect attempts at unauthorized access;

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

88. Thus, 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.

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

90. 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.

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

92. 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 and Class members' PII.

93. 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 the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class members' sensitive PII.

94. 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.

95. 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.

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

97. 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.

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

99. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff 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.

100. 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 and Class members' injury.

101. 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.

102. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

103. 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.

104. 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)

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

106. 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.

107. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for employment.

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

109. 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.

110. After all, Plaintiff and Class Members would not have entrusted their PII to Defendant or its third-party agents in the absence of such an agreement with Defendant.

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

112. 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.

113. 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.

114. 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.

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

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

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

THIRD CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

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

119. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

120. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

121. Because of the highly sensitive nature of the PII, Plaintiff and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

122. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff and Class members' PII.

123. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

124. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

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

126. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

127. Defendant owed a duty to its current and former clients, including Plaintiff and the Class, to keep this information confidential.

128. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class members' PII is highly offensive to a reasonable person.

129. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did

so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

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

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

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

134. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed supra).

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

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

137. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

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

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

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

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

141. 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.

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

143. 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.

144. 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.

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

146. 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.

SIXTH CAUSE OF ACTION
Violation of Florida Deceptive and Unfair Trade Practices Act
Fla. Stat. §§ 501.201, *et seq.*
(On Behalf of Plaintiff and the Class)

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

148. This cause of action is brought under the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA").

149. The purpose of FDUTPA is to "protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.202(2).

150. Another purpose of FDUTPA is to construe consumer protection as "consistent with established policies of federal law relating to consumer protection." Fla. Stat. § 501.202(3).

151. Plaintiff and Class members all constitute "[c]onsumers" under FDUTPA because they are all "individual[s]." Fla. Stat. § 501.203.

152. Plaintiff and Class members each constitute an "[i]nterested party or person" under FDUTPA because they are all "affected by a violation" of FDUTPA. Fla. Stat. § 501.203.

153. FDUTPA applies to Defendant because Defendant engages in "[t]rade or commerce" as defined as "advertising, soliciting, providing, offering, or distributing, whether by sale, rental, or otherwise, of any good or service, or any property, whether tangible or intangible, or any other article, commodity, or thing of value, wherever situated." Fla. Stat. § 501.203.

154. FDUTPA declares as unlawful "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.204(1).

155. FDUTPA provides that "due consideration be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a)(1) of the Trade Commission Act." Fla. Stat. § 501.204(2).

156. Relevant here, is that "[v]iolation[s]" of FDUTPA is broadly defined to include violations of:

a. "Any rules promulgated pursuant to the Federal Trade Commission Act, 15 U.S.C. ss. 41 *et seq.*" Fla. Stat. § 501.203.

b. "The standards of unfairness and deception set forth and interpreted by the Federal Trade Commission or the federal courts." Fla. Stat. § 501.203.

c. "Any law, statute, rule, regulation, or ordinance which proscribes unfair methods of competition, or unfair, deceptive, or unconscionable acts or practices." Fla. Stat. § 501.203.

157. Under FCRA, HIPAA (42 U.S.C. § 1302d *et seq.*), the FTCA, and Florida law (Fla. Stat. § 456.057 and § 501.171), Defendant was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class members' PII. Defendant was also under an obligation expressly under Florida law, where Defendant is headquartered and managed, to adequately protect Plaintiff's and Class members' PII.

158. Moreover, FDUTPA requires that Defendant (1) take reasonable measures to protect and secure data in electronic form containing PII; (2) take reasonable measures to dispose

of or destroy PII; and (3) provide notice to consumers and consumer reporting agencies subject to the FCRA when a data security incident occurs that compromises PII. Fla. Stat. §§ 501.171.

159. Defendant violated FDUTPA by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

160. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII.

161. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

162. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII that Plaintiff and Class members (or their third-party agents) entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

163. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class members' rights.

164. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

165. Plaintiff and Class members seek declaratory judgement that Defendant's practices were unreasonable and inadequate and thus caused the Data Breach.

166. Plaintiff and Class members seek injunctive relief enjoining the wrongful acts described *supra* and requiring Defendant to use and maintain proper standards for data security including, *inter alia*, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing. Fla. Stat. § 501.211(1).

167. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law. Plaintiff seeks actual damages, attorneys' fees, and costs under Fla. Stat. §§ 501.2105, 501.211(2).

PRAYER FOR RELIEF

Plaintiff and Class members respectfully request 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 representative, and appointing his 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. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

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

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

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

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

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

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: April 19, 2024

Respectfully submitted,

By: /s/*Joshua R. Jacobson*
Joshua R. Jacobson
Florida Bar No. 1002264
JACOBSON PHILLIPS PLLC
478 E. Altamonte Dr., Ste. 108-570
Altamonte Springs, FL 32701
Phone: 407-720-4057
jacob@jacobsonphillips.com
joshua@jacobsonphillips.com
eservice@jacobsonphillips.com

TURKE & STRAUSS LLP
Brittany Resch
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
brittanyr@turkestrauss.com

Attorneys for Plaintiff and Proposed Class