IN THE CIRCUIT COURT OF THE SIXTEENTH JUDICIAL CIRCUIT
KANE COUNTY, ILLINOIS

TYLER OLIVER, on behalf of himself and all others similarly situated, Plaintiff, v. **PARKSITE, INC.**, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED** 2025-CH-000056

Tyler Oliver ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Parksite, Inc. ("Parksite" 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 "wholesale supplier of premium interior and exterior building products specializing in project solutions, training, and education."[1] Defendant has 22 locations throughout the United States[2] and over 650 employee-owners.[3]

[1] *Home Page*, PARKSITE, https://www.parksite.com/ (last visited September 3, 2024).
[2] Locations, PARKSITE, https://www.parksite.com/locations/ (last visited September 3, 2024).
[3] About, PARKSITE, https://www.parksite.com/about/ (last visited September 3, 2024).

Please see page 33 for CMC

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") about its current and former employees and their beneficiaries. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. Upon information and belief, the cybercriminals had access to Defendant's network from December 25, 2023, until January 16, 2024—a shocking *23 days*—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 its current and former employees' and their beneficiaries' PII.

5. Defendant waited until May 24, 2024, to begin notifying victims—an appalling five months after the Breach began. A sample of Defendant's Breach Notice is attached as Exhibit A.

6. 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.

7. Plaintiff is a Data Breach victim. He brings this class action on behalf of himself, and all others harmed by Defendant's misconduct.

8. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former employees' and their beneficiaries' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

9. Plaintiff, Tyler Oliver, is a natural person and citizen of Connecticut. He resides in Lebanon, Connecticut where he intends to remain.

10. Defendant, Parksite, Inc., is a domestic corporation incorporated in Illinois and with its headquarters at 1563 Hubbard Ave., Batavia, Illinois 60510.

JURISDICTION AND VENUE

11. This Court has subject-matter jurisdiction over this action under Ill. Const. Art. VI, § 9.

12. This Court has personal jurisdiction over Defendant under 735 ILCS 5/2-209 because it is headquartered in Illinois, regularly conducts business in Illinois, and has sufficient minimum contacts in Illinois.

13. Venue is proper in this District under 735 ILCS 5/2-101(2) because Defendant's principal office is in this County, and because a substantial part of the events or omissions giving rise to the claim occurred in this County.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and the Class

14. Defendant "distributes category-leading building construction products and specialty building materials to dealers and fabricators within the commercial construction, residential construction, and remodeling markets."[4]

15. As part of its business, Defendant receives and maintains the PII of thousands of its current and former employees and their beneficiaries.

[4] *Id.*

16. 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.

17. Under state and federal law, businesses like Defendant have duties to protect its current and former employees' and their beneficiaries' PII and to notify them about breaches.

18. Defendant recognizes these duties, declaring in its "Privacy Policy" that it "take[s] steps to protect the information we collect about you."[5]

Defendant's Data Breach

19. On December 25, 2023, an unauthorized actor accessed Defendant's network. Defendant did not discover the Data Breach until January 16, 2024—over three weeks after the Data Breach began. Ex. A.

20. An internal investigation revealed that the unauthorized actor "may have accessed and removed certain files from our network environment." Ex. A.

21. Worryingly, Defendant admits that "certain files containing your personal information" were accessed *and/or acquired* by the unauthorized party. Ex. A.

22. Upon information and belief, Defendant's Data Breach impacted at least 7,886 individuals.[6] And upon information and belief, these 7,886 victims of the Data Breach include Defendant's current and former employees and their beneficiaries.

23. On or around May 3, 2024–five months after the Breach occurred – Parksite finally began notifying its employees about the Data Breach.

---

[5] Privacy Policy, PARKSITE https://www.parksite.com/privacy-policy/ (last visited September 3, 2024).

[6] Data Breach Notifications, MAINE OFFICE OF ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/17ecff1b-cdaa-40fb-acb9-584eb4859d7d.shtml (last visited September 3, 2024).

24. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing employees' PII, as evidenced by both the Data Breach.

25. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis" and to enroll in credit monitoring to "detect possible misuse of your personal information." Ex. A.

26. Defendant also recognized its duty to implement reasonable cybersecurity safeguards or policies to protect employees' PII, insisting that, despite the Data Breach demonstrating otherwise, "[t]he privacy and security of the personal information we maintain is of the utmost importance to Parksite[.]" Ex. A.

27. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

28. On information and belief, Parksite has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

29. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

30. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they suffered and will suffer.

31. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

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.

33. Worryingly, the cybercriminals that obtained Plaintiff's and Class members' PII appear to be the notorious ransomware group "Cactus"—which has been targeting "large commercial entities since March 2023."[7] As with many ransomware groups, Cactus attempt[s] to exfiltrate sensitive data to increase the pressure of extortion."[8]

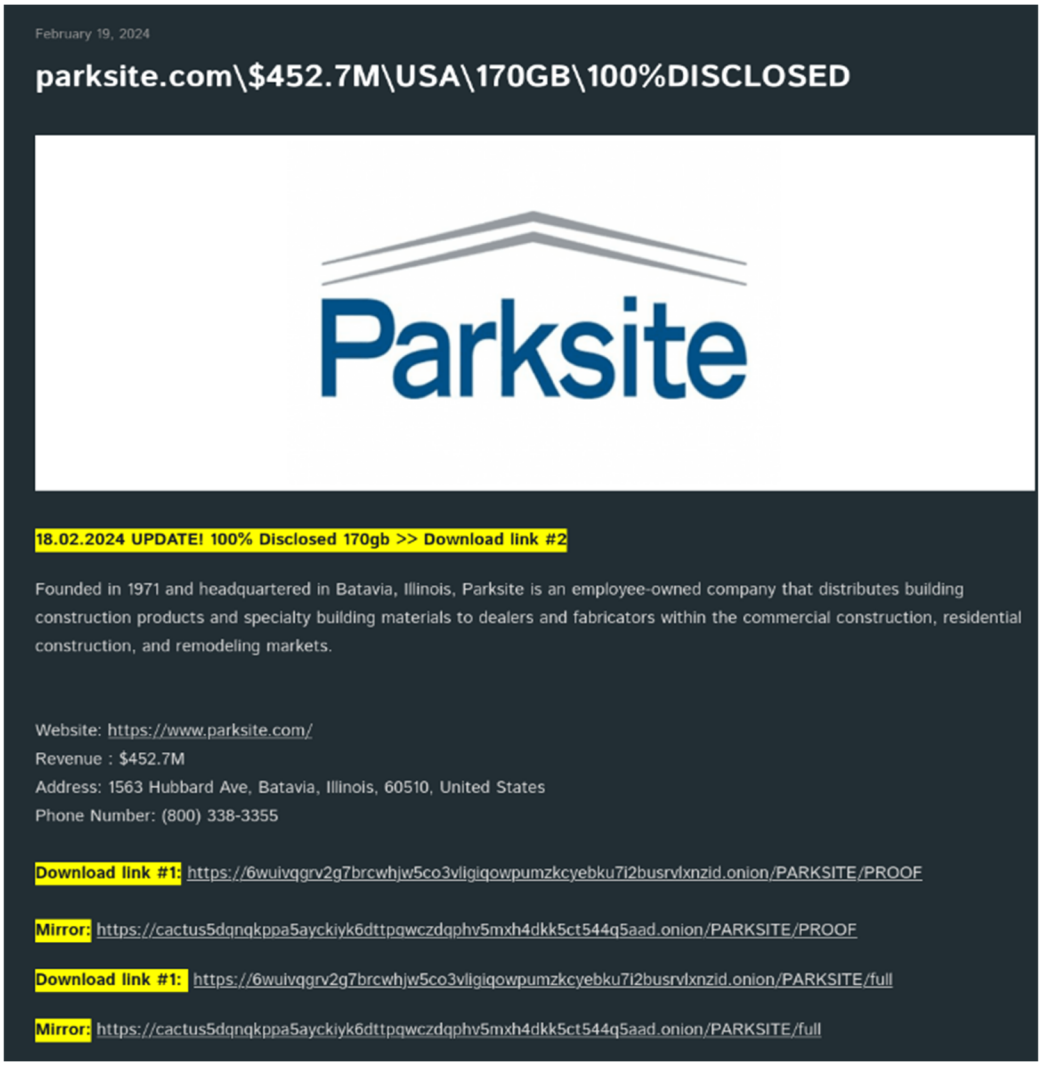
[7] CACTUS Ransomware: Prickly New Variant Evades Detection, KROLL, https://www.kroll.com/en/insights/publications/cyber/cactus-ransomware-prickly-new-variant-evades-detection (last visited September 4, 2024).
[8] *Id.*

34. On or around February 9, 2024, Cactus claimed credit for the Data Breach, stating that it had acquired and disclosed 170 GB of company data.[9]

35. Later, on February 19, 2024, Cactus updated its post, providing links to the exfiltrated data as well as screenshots of the data. The screenshots included financial information, Social Security cards, and employee tax forms, which included employees' Social Security numbers, dates of birth, full names, contact information, and addresses.[10]

[9] @FalconFeeds.io, TWITTER (X) (February 9, 2024, 6:30 AM) https://x.com/FalconFeedsio/status/1755932058281447532/photo/1 (last visited September 3, 2024).

[10] RANSOM LOOK, https://www.ransomlook.io/screenshots/cactus/parksitecom%5C%244527M%5CUSA%5C170GB%5C100%25DISCLOSED.png (last visited September 3, 2024).



36. As the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[11]

37. Thus, on information and belief, Plaintiff's and the Class's stolen PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiff's Experiences and Injuries

[11] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

38. Plaintiff Tyler Oliver's father is a former employee of Defendant, and Plaintiff is a beneficiary.

39. Thus, Defendant obtained and maintained Plaintiff's PII. And as a result, Plaintiff was injured by Defendant's Data Breach.

40. 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.

41. Plaintiff reasonably understood that a portion of the funds derived from employees' employment would be used to pay for adequate cybersecurity and protection of PII.

42. Upon information and belief, through its Data Breach, Defendant compromised Plaintiff's PII. And upon information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

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

44. 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.

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

46. 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.

47. 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.

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

49. 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

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.).

55. 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.

56. 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.

57. 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.

58. 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

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

60. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[12] The 330 reported breaches reported in 2021 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.[13]

61. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [14]

62. Cyberattacks on manufacturing companies like Defendant have become extremely notorious in recent years, with manufacturing firms suffering more than 130 data breaches, exposed 38 million records, in 2022.[15] Further, "since 2020, US businesses that specialize in manufacturing and utilities have suffered 973 data breaches affecting more than 202 million records."[16]

63. 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.

---

[12] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited August 26, 2024).

[13] *Id*.

[14] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited August 26, 2024).

[15] Inside the Breach: Why & How Manufacturers are Compromised, ProcessUnity, https://www.processunity.com/inside-the-breach-why-and-how-manufacturers-are-compromised/ (last visited August 26, 2024).

[16] US manufacturing & utility businesses leaked nearly 88 million records in 302 data breaches in 2023, Comparitech,, https://www.comparitech.com/blog/vpn-privacy/us-manufacturing-utility-breaches/ (last visited August 26, 2024).

Defendant Failed to Follow FTC Guidelines

64. 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.

65. 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.[17] 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.

66. 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.

67. 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

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

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

68. 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.

69. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former employees' and their beneficiaries' 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

70. 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.

71. 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.

72. 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.

73. 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

74. Plaintiff hereby incorporates by reference and re-alleges herein the allegations contained in all preceding paragraphs of this Complaint.

75. Plaintiff brings this action as a class action pursuant to 735 ILCS 5/2-801.

76. Plaintiff seeks to represent the following class (the "Class"):

> All individuals residing in the United States whose PII was compromised in the Data Breach discovered by Parksite in January 2024, including all those individuals who received notice of the breach.

77. 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.

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

79. 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.

735 ILCS § 5/2-801(1) Numerosity

80. The Class is so numerous that joinder of all Class members is impracticable.

81. Upon information and belief, the proposed Class includes at least 2,652 members.

735 ILCS § 5/2-801(2) Commonality & Predominance

82. The claims of Plaintiff and the Class Members raise common factual and legal questions that predominate over any individual issues which may affect the Class and for which a class wide proceeding is the most efficient means to resolve these questions 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.

83. 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.

735 ILCS § 5/2-801(3) Adequacy

84. Plaintiff will fairly and adequately protect the common interests of the proposed Class. Their interests do not conflict with those of the Class Members. Moreover, Plaintiff have retained experienced counsel, who specialize in complex class action litigation and data privacy, to prosecute this action on behalf of the Class.

735 ILCS 5/2-801(4) Appropriateness

85. A class action is appropriate and 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)

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

87. 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.

88. 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.

89. 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.

90. 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.

91. 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.

92. 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.

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

94. 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.

95. 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 services from Defendant.

96. 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.

97. 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.

98. 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.

99. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant hold 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 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 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 because 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. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

109. 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)

110. Plaintiff and Class members either directly contracted with Defendant or Plaintiff and Class members were the third-party beneficiaries of contracts with Defendant.

111. Plaintiff and Class members (or their third-party agents) were required to provide their PII to Defendant as a condition of receiving products, services, and/or employment provided by Defendant. Plaintiff and Class members (or their third-party agents) provided their PII to Defendant in exchange for Defendant's employment.

112. Plaintiff and Class members (or their third-party agents) reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

113. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

114. Plaintiff and the Class members (or their third-party agents) accepted Defendant's offers by disclosing their PII to Defendant in exchange for employment.

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

116. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII.

117. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their PII.

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

119. Plaintiff and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendant.

120. 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.

121. 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.

122. Defendant materially breached the contracts it entered with Plaintiff and Class members (or their third-party agents) 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.

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

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

125. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

126. Plaintiff and Class members (or their third-party agents) 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)

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

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

129. Plaintiff and Class members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to facilitate employment and its business.

130. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members (or their third-party agents).

131. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

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

133. 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.

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

135. Plaintiff and Class members have no adequate remedy at law.

136. 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
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

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

138. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's 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.

139. 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.

140. Because of the highly sensitive nature of the PII, Plaintiff and Class members (or their third-party agents) 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.

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

142. 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.

143. 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*).

FIFTH CAUSE OF ACTION
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 ICLS 505/1, *et seq*.
(On Behalf of Plaintiff and the Class)

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

145. This claim is brought under the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA").

146. Plaintiff and Class members are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e).

147. Plaintiff, the Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

148. The ICFA applies to Defendant because Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

149. Defendant violated ICFA 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*.

150. 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.

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

152. Had Defendant disclosed to Plaintiff and Class members (or their third-party agents) 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.

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

154. 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.

155. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

156. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law.

157. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiff and the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

158. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Class of the nature and extent of the Data Breach pursuant to the Illinois PII Protection Act, 815 ILCS 530/1, *et seq*.

159. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the ICFA.

SIXTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

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

161. 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.

162. 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

alleges 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.

163. 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.

164. 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.

165. 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.

166. 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 and Class members' injuries.

167. 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.

168. 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 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 unfair and/or deceptive practices;

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.

Dated: May 6, 2025

Respectfully Submitted,

By: /s/ *Cassandra P. Miller*

Cassandra P. Miller
Stephen J. Pigozzi
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
cmiller@straussborrelli.com
spigozzi@straussborrelli.com

Counsel for Plaintiff and the Proposed Class

ClassAction.org