UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

SEATTLE DIVISION

NATHAN BAKER, on behalf of himself and all others similarly situated, Plaintiff, v. **DOLLY, INC.**, Defendant.	Case No. 2:23-cv-02004 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Nathan Baker ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Dolly, Inc. ("Dolly" 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

2. Defendant is a delivery service business that is "currently operating in 45 cities, expanding quickly, and will soon be nationwide."[1] It advertises 3.2 million items delivered and 15,000 "[h]elpers ready to lend a hand."[2]

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") about its current and former employees, independent contractors, and customers. But Defendant lost control over that 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 its current and former employees, independent contractors, and customers' 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—attached as Exhibit A. 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, its current and former employees, independent contractors, and customers' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

---

[1] *About*, DOLLY, https://dolly.com/about (last visited Dec. 28, 2023).
[2] *Id*.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

PARTIES

8. Plaintiff Nathan Baker is natural person and citizen of Wisconsin. He resides in Marshfield, Wisconsin where he intends to remain.

9. Defendant, Dolly, Inc., is a Foreign Profit Corporation incorporated in Delaware with its principal place of business at 901 Fifth Avenue, Suite 600, Seattle, Washington 98164.

JURISDICTION AND VENUE

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

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

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

BACKGROUND

Defendant Collected and Stored the PII of Plaintiff and the Class

13. Defendant is a delivery service business that is "currently operating in 45 cities, expanding quickly, and will soon be nationwide."[3] It advertises 3.2 million items delivered and 15,000 "[h]elpers ready to lend a hand."[4]

14. As part of its business, Defendant receives and maintains the PII of thousands of its current and former employees, independent contractors, and customers.

[3] *About*, DOLLY, https://dolly.com/about (last visited Dec. 28, 2023).
[4] *Id*.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

15. 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.

16. Under state and federal law, businesses like Defendant have duties to protect its current and former employees, independent contractors, and customers' PII and to notify them about breaches.

17. Defendant recognizes these duties, declaring in its "Dolly Privacy Policy" that:

a. "At Dolly, Inc. ('Dolly'), we appreciate the trust you place in us when you choose to visit our website and we take that responsibility seriously."[5]

b. "This Dolly Privacy Policy (the 'Policy') describes how we collect and use personal information about you when you visit our website, use our mobile application, or call us on the phone."[6]

c. "In general, we do not share personal information about you with third parties."[7]

d. "We retain your Personal Information for the length of time required for the specific purpose or purposes for which it was collected and we will securely delete that information once we no longer need it."[8]

e. "Dolly will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice."[9]

f. "When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep

---

[5] *Dolly Privacy Policy*, DOLLY (Feb. 10, 2020) https://dolly.com/privacy.
[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

that personal information confidential and not use it for any purpose except performing the contract."[10]

18. Moreover, Defendant's "Dolly Privacy Policy" reveals that it collects and maintains a very broad range of personal information including, *inter alia*:

a. "Contact information, such as your name, address, phone number, or email address;"

b. "Purchase information, such as the items you purchase, payment method and payment information (such as debit or credit card number and information), billing and shipping address, and contact information (such as for receipts or order updates);"

c. "Profile and account information, which may include Contact, Purchase, and Preference information as well as your account password, and other information about your profile or account;"

d. "Demographic information, which may include age or birthdate, gender, ZIP code, and other information about you;"

e. "Call recordings including information about your call and that you share when you call us on the phone;"

f. "Location information of your device that you use with our mobile application, if your device settings allow us to collect location information;" and

g. "Device and browsing information, including information about your phone, tablet, computer, or device, and online browsing activity (collectively, 'automatically collected information'). Automatically collected information may include IP addresses, unique device identifiers,

[10] *Id.*

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

> cookie identifiers, device and browser settings and information, and Internet service provider information. Automatically collected information also may include information about when and how you access and use our website or mobile application, such as the date and time of your visit or use, the websites you visit before coming and after leaving our website, how you navigate and what you search for using our website and mobile application, the website pages and items you view using our website and mobile application, and the items you purchase."[11]

Defendant's Data Breach

19. On August 26, 2023, Defendant noticed that it was hacked.[12] But it is unclear when the hack began. Thus, on information and belief, the Data Breach began before August 26, 2023.

20. Worryingly, Defendant already admitted that "an unknown criminal actor *acquired* certain files from our network, some of which contained individuals' personal information."[13]

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

a. names; and

b. Social Security numbers.[14]

22. But upon information and belief, Defendant's Data Breach exposed a far greater range of types of PII. After all, as explained *supra*, Defendant collects and maintains a variety of personal information. Thus, upon information and belief, the Data Breach also exposed:

a. addresses;

---

[11] *Id*.
[12] *Notification Letter*, DEPT JUSTICE MONTANA, https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-815.pdf (last visited Dec. 28, 2023).
[13] *Id*. (emphasis added).
[14] *Id*.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

b. phone numbers;

c. email addresses;

d. debit and credit card numbers and information;

e. ages;

f. birthdates;

g. genders;

h. call recordings;

i. location information;

j. device and browsing information;

k. IP addresses;

l. unique device identifiers;

m. cookie identifiers;

n. device and browser settings and information; and

o. internet service provider information.[15]

23. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendant's custody and control. And upon information and belief, the putative class is over one hundred members—as it includes its current and former employees, independent contractors, and customers.

24. And yet, Defendant waited over until November 2, 2023, before it began notifying the class—a full sixty-eight (68) days after the Data Breach was discovered.[16]

25. 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.

[15] *See Dolly Privacy Policy*, DOLLY (Feb. 10, 2020) https://dolly.com/privacy.
[16] *Id*.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

26. 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:

a. "remain vigilant by reviewing your account statements and credit reports closely;"

b. "enroll in the IDX identity protection services;"

c. "report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC);" and

d. "obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft."[17]

27. 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.

28. Since the breach, Defendant has "implemented measures to enhance our network security."[18] 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.

---

[17] *Id.*

[18] *Id.*

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

31. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims 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.

33. Worryingly, the cybercriminals that obtained Plaintiff's and Class members' PII appear to have leaked the stolen PII on the Dark Web.[19] Specifically, various news outlets have reported the following:

a. "Dolly.com, an on-demand moving and delivery platform, allegedly paid attackers not to publish stolen customer data."[20]

b. "Dolly.com . . . suffered a ransomware attack and at least partially paid the ransom."[21]

c. "The attackers complained that the payment wasn't generous enough and published the stolen data."[22]

d. "Not only that, but the criminals also shared a chat with the company on an underground criminal forum."[23]

---

[19] Vilius Petkauskas, *Dolly.com pays ransom, attackers release data anyway*, CYBERNEWS (November 15, 2023, 12:53 PM) https://cybernews.com/security/dolly-data-breach-ransomware-attack/.

[20] *Id*.

[21] *Id*.

[22] *Id*.

[23] *Id*.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

e. "Attackers posted details about the Dolly.com hack on a notorious Russian-language forum, typically employed by ransomware operators and stolen data traders."[24]

f. "One of the emails between the attackers and the victim, dated September 7th, showed that Dolly.com agreed to pay the ransom."[25]

g. "[A]ttackers said they had access to the entire credit card data."[26]

h. "[T]he attackers uploaded the data and posted two download links on a forum infested with cybercriminals."[27]

34. Most concerningly, is that it appears that "the cybercriminals obtained sensitive company and customer data" including:

a. high-level account login details;

b. credit card information;

c. customer addresses;

d. names;

e. registration dates;

f. user emails; and

g. system data.[28]

35. Thus, it appears that the types of PII exposed were extremely broad and especially sensitive—in sharp contrast to Defendant's statements that only names, and Social Security numbers were exposed.

36. And 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

---

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[29]

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

38. Plaintiff Nathan Baker is a former employee of Defendant—having worked as a driver and mover in or around 2019 and 2020.

39. Thus, Defendant obtained and maintained Plaintiff's PII.

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

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

42. 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.

43. Plaintiff reasonably understood that a portion of the funds paid to Defendant (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of PII.

44. Plaintiff received a Notice of Data Breach dated November 2, 2023—attached as Exhibit A.

[29] 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

46. Through its Data Breach, Defendant compromised Plaintiff's:

a. name; and

b. Social Security number.

47. Plaintiff has *already* spent several hours (1) carefully reviewing his accounts, and (2) placing credit freezes on his accounts.

48. Plaintiff will continue to spend significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

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

50. 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.

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

52. 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.

53. 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

55. 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

56. 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

57. 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.

58. 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.

59. 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.

60. 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.).

61. 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.

62. 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.

63. 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

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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.

64. 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

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

66. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[30]

67. 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."[31]

68. 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

69. 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

---

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

[31] 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

70. 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.[32] 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.

71. 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.

72. 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.

73. 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"),

[32] *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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

74. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former employees, independent contractors, and customers' 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

75. 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.

76. 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.

77. 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

78. 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

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

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

80. 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.

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

82. 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.

83. 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.

84. 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 one hundred members.

85. 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

86. 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.

87. 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.

88. 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

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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)

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

90. 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.

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

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

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

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

94. 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.

95. 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.

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

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

98. Defendant's duty to use reasonable security measures arose 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

99. 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.

100. 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.

101. 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.

102. 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.

103. 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.

104. 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.

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

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

106. 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.

107. 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.

108. 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.

109. 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.

110. 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.

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

112. 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

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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)

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

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

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

116. Plaintiff and Class members reasonably understood that a portion of the funds they paid Defendant (or the funds that Defendant derived from their labor) would be used to pay for adequate cybersecurity measures.

117. Plaintiff and Class members 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.

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

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

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

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

121. 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.

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

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

124. 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.

125. 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.

126. 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

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

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

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

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

130. 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)

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

132. 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.

133. 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.

134. 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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

136. 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.

137. 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)

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

139. 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.

140. Defendant owed a duty to its current and former employees, independent contractors, and customers, including Plaintiff and the Class, to keep this information confidential.

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

142. 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

143. The Data Breach constitutes an intentional interference with Plaintiff's 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.

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

145. 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.

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

147. 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*).

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

149. 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.

150. 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

151. 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)

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

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

154. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to provide services and/or facilitate employment.

155. 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 provide services and/or facilitate employment.

156. Plaintiff and Class members 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.

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

158. 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

159. 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.

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

161. 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 Washington Consumer Protection Act
RCW 19.86.010, *et seq*.
(On Behalf of Plaintiff and the Class)

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

163. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

164. Defendant is a "person" as described in RWC 19.86.010(1).

165. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

166. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

167. Defendant's failure to safeguard the PII exposed in the Data Breach constitutes an unfair act that offends public policy.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

168. Defendant's failure to safeguard the PII exposed in the Data Breach constitutes an unfair act that offends public policy.

169. Defendant's failure to safeguard the PII compromised in the Data Breach caused substantial injury to Plaintiff and Class Members. Defendant's failure is not outweighed by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.

170. Defendant's failure to safeguard the PII disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

171. In the course of conducting its business, Defendant committed "unfair or deceptive acts or practices" by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

172. Defendant also violated the CPA by failing to timely notify, and by concealing from Plaintiff and Class Members, information regarding the unauthorized release and disclosure of their PII. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII and identities.

173. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

174. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

175. Defendant's unfair or deceptive acts or practices occurred in its trade or business and have injured and are capable of injuring a substantial portion of the public. Defendant's general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

176. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CPA, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII; (5) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

177. Unless restrained and enjoined, Defendant will continue to engage in the wrongful conduct (detailed *supra*) and more data breaches will occur. Plaintiff, therefore, on behalf of themselves and the Class, seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies,

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it.

178. Plaintiff, on behalf of himself and Class Members, also seek to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff, on behalf of himself and Class Members, request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained not to exceed $25,000.00 per Class Member.

SEVENTH CAUSE OF ACTION
Data Breach Notification Disclosure Law. § 19.255.005
(On Behalf of Plaintiff and the Class)

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

180. Under RCW § 19.255.010(2), "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

181. Upon information and belief, this statute applies to Defendant because Defendant does not own nor license the PII in question. Instead, the owners and/or licensees of the PII are Plaintiff and the Class.

182. Here, the Data Breach led to "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendant, leading to a "breach of the security of [Defendant's] systems," as defined by RCW § 19.255.010.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

183. Defendant failed to disclose that the PII—of Plaintiffs and Class Members— that had been compromised "immediately" upon discovery, and thus unreasonably delayed informing Plaintiffs and the proposed Class about the Data Breach.

184. Thus, Defendant violated the Washington Data Breach Disclosure Law.

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

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

186. 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.

187. 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.

188. 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.

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

189. 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.

190. 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.

191. 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.

192. 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.

193. 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;

TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703-3515
TEL. 608.237.1775 • FAX 608.509.4423
www.turkestrauss.com

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: December 29, 2023

By: */s/ Samuel J. Strauss*

Samuel J. Strauss, WSBA #46971
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703-3515
Telephone: (608) 237-1775
Facsimile: (608) 509 4423
sam@turkestrauss.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org
