E-FILED
Friday, 02 September, 2022 01:19:20 PM
Clerk, U.S. District Court, ILCD

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS
PEORIA DIVISION

CLARA OWENS, on behalf of herself and all others similarly situated, Plaintiff, v. AFNI, INC., Defendant.	Case No. 1:22-cv-01297 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Clara Owens, through her attorneys, brings this Class Action Complaint against the Defendant, Afni, Inc. ("Afni" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, alleging as follows:

INTRODUCTION

1. In June 2021, Afni, a worldwide debt collections company, lost control over individuals' highly sensitive personal information in a data breach by cybercriminals ("Data Breach").

2. The Data Breach exposed the highly sensitive "personally identifiable information" ("PII") belonging to over 261,000 individuals, including Afni employees, exposing their names, addresses, Social Security numbers, and financial account information.

3. But Afni would not tell breach victims about the Data Breach until June 2022, leaving them in the dark about the breach until over one year after it happened.

4. On information and belief, Afni allowed the hack to happen because it does not implement adequate cybersecurity to safeguard its employees and individuals' data. This is even though Afni recognizes that "[r]isk management and information security are more critical than ever[,]"[1] promising to remain "committed to providing the highest level of safety and security [for] our clients and employees."[2]

5. Afni's misconduct violates Illinois law, not only because it failed to protect individuals' PII, but also because Afni withheld notifying them about the breach for over one year.

6. In that time, breach victims were unaware that cybercriminals had stolen their PII and could misuse it, exposing them to a substantial risk of identity theft, including Plaintiff, who suffered identity theft following the breach.

7. Plaintiff is a former Afni employee and Data Breach victim. Since the Data Breach occurred in June 2021, Plaintiff's identity has been stolen to commit unemployment insurance fraud.

8. And when Afni finally notified Plaintiff and the class about the Data Breach in June 2022, it obfuscated its nature and downplayed the threat to victims, telling them that hackers only "may" have viewed or stolen their data and that Afni was only notifying them about the breach "out of an abundance of caution."

9. Its notice also did not clarify whether victims' information was irretrievably lost, whether the breach was a ransomware event, whose PII was accessed and stolen, whether Afni

[1] *See* Afni's website article announcing its new Chief Information Security Officer https://afni.com/news/2022/introducing-our-new-ciso (last visited Aug. 23, 2022).

[2] *See* Afni's blog post entitled "SAFE & SECURE" https://afni.com/news/case-studies/2022/safe-and-secure-at-home (last visited Aug. 23, 2022).

had improved its cybersecurity following the attack to protect PII, or why it took Afni one year to issue a bare-bones notice to its victims.

10. Worse, Afni's breach notice ("Breach Notice")[3] withheld key information about the breach, including that it had exposed victims' "Financial Account Number or Credit/Debit Card Number[s] (in combination with security code, access code, password or PIN for the account)[.]"[4]

11. In other words, cybercriminals had accessed all information necessary to immediately steal victims' identities during the Data Breach but did not tell them about that threat for over one year.

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

13. Plaintiff brings this Class Action on behalf of herself and all others harmed by Afni's misconduct.

PARTIES

14. Plaintiff is a natural person and citizen of Illinois, where she intends to remain. Plaintiff is a former Afni employee and Data Breach victim, receiving Afni's Breach Notice in July 2022.

15. Defendant, Afni, is an Illinois corporation, with its principal place of business at 1310 Martin Luther King Jr Dr., Bloomington, IL 61701.

[3] *See* Afni's Breach Notice attached as Exhibit A.

[4] *See* Afni's regulatory report to the Office of the Maine Attorney General attached as Exhibit B.

JURISDICTION & VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

17. This Court has personal jurisdiction over Defendant because is incorporated in Illinois, its principal place of business is in Illinois, and it does substantial business in Illinois.

18. Venue is proper in this District because Defendant is headquartered in this District, maintains its principal place of business in this district, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND FACTS

A. Afni

19. In business since 1930, Afni is a worldwide debt collector, providing customers consumer collections, insurance subrogation, and call center services.[5]

20. Afni currently employs around 9,000 individuals worldwide.

21. As a condition of employment, Afni requires its employees to disclose their PII, including their names, addresses, Social Security numbers, and financial account information.

22. On information and belief, Afni also collects individuals' PII in the normal course of its business, no matter whether they are Afni employees.

23. When Afni collects this information, it promises to use reasonable measures to safeguard PII from theft and misuse.

[5] *See* Afni's "What We Do" page, https://afni.com/what-we-do (last visited Aug. 23, 2022).

24. In fact, Afni explains that the "confidentiality, privacy, and security of information in our care are among [its] highest priorities," and advertises that it protects employee and customer data with the "highest level of safety and security":

> We didn't stop there. To improve our security prevention and mitigation results continually and proactively, Afni invested in additional industry-leading software on its endpoint to monitor, prevent, and respond to security incidents. We have also established a hybrid incident response team and third-party managed 24x7x365 security operations center. Afni remains committed to providing the highest level of safety and security four our clients and employees.

25. Indeed, Afni's Chief Executive Officer notes "[r]isk management and information security are more critical than ever[.]"[6] And its Chief Information Security Officer warns: "The simple fact of the matter is that, for most organisations globally, the threat posed by cyberattacks is among the top business risks in financial terms," meaning "the most likely extinction level threat for many firms comes from cyberattacks."

26. But despite understanding the importance of securing PII, on information and belief, Afni does not follow industry standard practices in securing PII, adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems.

27. As a result, Afni leaves PII an unguarded target for theft and misuse.

B. Afni Fails to Safeguard PII

28. Afni collects and maintains PII in its computer systems.

29. In collecting and maintaining the PII, Afni agreed it would safeguard the data according to its internal policies and state and federal law.

[6] *See* Afni's website article announcing its new Chief Information Security Officer https://afni.com/news/2022/introducing-our-new-ciso (last visited Aug. 23, 2022); *See* Afni's blog post "Security as a business enabler," https://afni.com/media/img/Security-as-Business-Enabler.pdf (last visited Aug. 23, 2022).

30. In June 2021, cybercriminals bypassed Afni's security systems and accessed its individuals' PII.

31. Although Afni eventually "identified suspicious activity" in its systems, it was unable to prevent, detect, or stop cybercriminals from accessing information on victims' names, addresses, Social Security numbers, and financial account information.

32. Following the attack, local news sources reported on the breach, but Afni refused to comment, leaving its victims in the dark about the Data Breach.[7]

33. Indeed, Afni would not notify impacted individuals about the breach for over one year.

34. In that time, Afni "investigated" the breach while individuals were exposed to identity theft, depriving breach victims of the earliest opportunity to mitigate the Data Breach's negative effects on them.

35. Afni's investigation dragged on from June 2021 through June 2022, resulting in Afni's Breach Notice to victims, which revealed scant information on the hack.

36. Indeed, the Breach Notice disclosed little, withholding information on how the hack happened, whether it was a ransomware attack, whether Afni paid a ransom, whether victims' information is irretrievably lost, what Afni is doing to prevent another breach, and why it took over one year to issue a bare-bones notice.

37. The notice also downplayed the breach, telling victims that cybercriminals only "may" have accessed their information and that Afni was issuing the notice only out of an "abundance of caution."

[7] *See* WGLT's article "Afni Shuts Down Its Network After 'Suspicious Activities' Detected" https://www.wglt.org/local-news/2021-06-12/afni-shuts-down-its-network-after-suspicious-activities-detected (last visited Aug. 23, 2022).

38. The Breach Notice otherwise withheld key information on the breach, including that it included their financial account information.

39. On information and belief, Afni allowed the Data Breach to happen because it failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over PII. Afni's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that Afni cannot, or will not, determine the full scope of the Data Breach, as it has been unable to determine exactly what information was stolen and when.

C. Plaintiff's Experience

40. Plaintiff is a former Afni employee, working for the company from February 2005 to December 2005 and March 2006 through June 11, 2021.

41. As a condition of Plaintiff's employment, Afni required Plaintiff to provide her PII.

42. Plaintiff provided her PII to Afni and trusted that the company would use reasonable measures to protect it according to Afni's internal policies and state and federal law.

43. Following the Data Breach, but before Afni disclosed it, Plaintiff suffered identity theft.

44. In June 2021, after the Data Breach occurred, an unemployment insurance claim was filed in her name without her authorization. Plaintiff was recently unemployed and had recently submitted an unemployment claim. Plaintiff never received any payments from the claim but the person who filed the claim received payment due to the fraudulent claim.

45. Plaintiff has also received an uptick in spam texts and phone calls following the breach.

46. Plaintiff has and will spend considerable time and effort monitoring her accounts

to protect herself from additional identity theft. To date, she has spent around more than 50 hours dealing with the identity theft.

D. Plaintiff and the Proposed Classes Face Significant Risk of Continued Identity Theft

47. Plaintiff and members of the proposed Classes have suffered injury from the misuse of their PII that can be directly traced to Defendant.

48. As a result of Afni's failure to prevent the Data Breach, Plaintiff and the proposed Classes have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

49. 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.

50. The value of Plaintiff and the proposed Classes' PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

51. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

52. One such example of criminals using PII for profit is the development of "Fullz" packages.

53. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

54. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Classes' phone numbers, email addresses, and other unregulated sources and identifiers. 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 members of the proposed Classes, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Classes' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

55. Defendant disclosed the PII of Plaintiff and members of the proposed Classes for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Classes 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.

56. Defendant's failure to properly notify Plaintiff and members of the proposed Classes of the Data Breach exacerbated Plaintiff and members of the proposed Classes' 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.

E. Defendant failed to adhere to FTC guidelines.

57. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

58. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal 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.

59. The guidelines also recommend that businesses watch for large amounts of data

being transmitted from the system and have a response plan ready in the event of a breach.

60. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

63. Plaintiff sues on behalf of themself and the proposed class and subclass (together, "Classes"), defined as follows:

> **Nationwide Class**: All individuals residing in the United States whose PII was compromised in the Data Breach.
>
> **Employee Subclass**: All individuals residing in the United States who are current or former Afni employees whose PII was compromised in the Data Breach.

Excluded from the Classes 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.

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

65. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the proposed Classes, consisting of 261,000 members, far too many to join in a single action;

b. **Ascertainability**. Members of the Classes are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of members of the Classes 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.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Classes' interests. Their interests do not conflict with Classes' interests and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Classes' behalf, including as lead counsel.

e. **Commonality**. Plaintiff and the Classes' claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all members of the Classes. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff and the Classes' PII;

ii. Whether 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;

iii. Whether Defendant was negligent in maintaining, protecting, and

securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff and the Classes' PII;

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

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff and the Classes injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Classes are entitled to damages, treble damages, or injunctive relief.

66. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and all Classes)

67. Plaintiff reallege all previous paragraphs as if fully set forth below.

68. Plaintiff and members of the Classes entrusted their PII to Defendant. Defendant owed to Plaintiff and other members of the Classes a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

69. Defendant owed a duty of care to Plaintiff and members of the Classes because it

was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and members of the Classes' PII by disclosing and providing access to this information to third parties and by 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.

70. Defendant owed to Plaintiff and members of the Classes a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Classes the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Classes 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.

71. Defendant owed these duties to Plaintiff and members of the Classes 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 protocols. Defendant actively sought and obtained Plaintiff' and members of the Classes' personal information and PII.

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

73. 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 members of the Classes' and the importance of exercising reasonable care in handling it.

74. 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 members of the Classes which actually and proximately caused the Data Breach and Plaintiff and members of the Classes' injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Classes, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and members of the Classes' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Classes have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

75. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Classes 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.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and all Classes)

76. Plaintiff and members of the Classes incorporate the above allegations as if fully

set forth herein.

77. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Classes' PII.

78. 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 individuals' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Classes' sensitive PII.

79. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect individuals' 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 its individuals in the event of a breach, which ultimately came to pass.

80. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Classes.

81. Defendant had a duty to Plaintiff and the members of the Classes to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Classes' PII.

82. Defendant breached its respective duties to Plaintiff and members of the Classes under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Classes' PII.

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

84. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Classes, Plaintiff and members of the Classes would not have been injured.

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

86. Had Plaintiff and members of the Classes known that Defendant did not adequately protect their PII, Plaintiff and members of the Classes would not have entrusted Defendant with their PII.

87. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Classes have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiff and the Employee Subclass)

88. Plaintiff and members of the Employee Subclass incorporate the above allegations as if fully set forth herein.

89. Defendant offered to employ Plaintiff and members of the Employee Subclass in exchange for their PII.

90. In turn, and through internal policies, Defendant agreed it would not disclose the PII it collects to unauthorized persons. Defendant also promised to safeguard employee PII.

91. Plaintiff and the members of the Employee Subclass accepted Defendant's offer by providing PII to Defendant in exchange for employment with Defendant.

92. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Employee Subclass with prompt and adequate notice of all unauthorized access and/or theft of their PII.

93. Plaintiff and the members of the Employee Subclass would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

94. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Employee Subclass by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Employee Subclass by:

a. Failing to properly safeguard and protect Plaintiff and members of the Employee Subclass's PII;

b. Failing to comply with industry standards as well as legal obligations that

are necessarily incorporated into the parties' agreement; and

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

95. The damages sustained by Plaintiff and members of the Employee Subclass as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

96. Plaintiff and members of the Employee Subclass have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

97. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The 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—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

99. Defendant failed to advise Plaintiff and members of the Employee Subclass of the Data Breach promptly and sufficiently.

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

101. Plaintiff and members of the Employee Subclass have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the

covenant of good faith and fair dealing.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Employee Subclass)

102. Plaintiff and members of the Employee Subclass incorporate the above allegations as if fully set forth herein.

103. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

104. Plaintiff and members of the Employee Subclass conferred a benefit upon Defendant in the form of services through employment.

105. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Employee Subclass. Defendant also benefited from the receipt of Plaintiff and members of the Employee Subclass's PII, as this was used to facilitate their employment.

106. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Employee Subclass's services and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Employee Subclass would not have provided their PII or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their PII.

107. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Employee Subclass all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

PRAYER FOR RELIEF

Plaintiff and members of the Classes demand a jury trial on all claims so triable and request that the Court enter an order:

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

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Classes;

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

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Classes damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Classes 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 Classes leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: September 2, 2022

Respectfully submitted,

By: */s/ Mary C. Turke*

Mary C. Turke
mary@turkestrauss.com
Samuel J. Strauss
sam@turkestrauss.com
Raina C. Borrelli
raina@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423

Attorneys for Plaintiff