E-FILED
Monday, 29 August, 2022 05:49:56 PM
Clerk, U.S. District Court, ILCD

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS

NICOLE PROCHNOW, individually and on behalf of all others similarly situated, Plaintiff, v. AFNI, INC., Defendant.	Case No. CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff, Nicole Prochnow, 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. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

INTRODUCTION

1. Afni, is an international company with over 9,000 employees that serves the healthcare, insurance, and communications industries and offers consumer debt collection, customer assistance and engagement, back-office management, and insurance subrogation services.

2. As a necessary and regular part of its business, Afni collects and maintains sensitive, nonpublic personally identifiable information of its employees and consumers.

3. In June 2021, Afni detected "anomalous activity within its computer network" and determined that it lost control over files containing highly sensitive personal information of at least 261,449 people during a breach of its network by a criminal actor ("Data Breach").

4. Afni waited over a year to inform the over 260,000 victims of the Data Breach that their names, dates of birth, Social Security numbers, and addresses ("PII") were exposed to criminals. Despite discovering the Data Breach in June 2021, Afni did not begin noticing Plaintiff and Class members until June 14, 2022, leaving them unable to take basic preventative measures to mitigate harm that resulted from the Data Breach.

5. Afni's failure to implement adequate cybersecurity to safeguard its employees' and consumers' PII left that PII in a vulnerable and dangerous condition and allowed the Data Breach to happen. Afni's failure to safe guard PII came despite its recognition that "[r]isk management and information security are more critical than ever[,]"1 and its promises to remain "committed to providing the highest level of safety and security [for] our clients and employees."2

6. Afni's misconduct violates Illinois law, not only because it failed to protect Plaintiff and Class Members' PII, but also because Afni withheld notifying them about the breach for over one year from the date on which it discovered the Data Breach.

7. For over a year, victims like Plaintiff and Class Members were unaware that cybercriminals had stolen their PII and could and did misuse it, exposing them to a substantial risk of, and actual, identity theft. Plaintiff, as an unfortunate example, suffered seven attempts at fraud or identity theft since the Data Breach occurred in June 2021.

8. Defendant's failure to timely notice Plaintiff and the Class is made all the more

[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).

egregious because it misleads victims as to the scope and severity of the Data Breach and its consequences. 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."3 The notice further downplays the threat to Plaintiff and Class Members by assuring them that Afni is "unaware of any actual or attempted identity theft or fraud" despite the fact that none of the victims of the Data Breach were aware that Afni had lost control of their PII and would not think to report any fraud to Afni.

9. Worse still, Afni's Notice withheld key information about the Data Breach. Afni reported to the Maine Attorney General that the Data Brech included "Financial Account Number or Credit/Debit Card Number[s] (in combination with security code, access code, password or PIN for the account),"4 but omitted this information from the Notice to Plaintiff and the Class.

10. The Notice also does not inform victims why it took Anfi 12 months to inform them of the Data Breach, the mechanism by which the attack happened, whether Anfi has implemented additional data security protocols or training, or whether Afni recovered the data.

11. Plaintiff and the Class were harmed by Afni's failure to implement proper data security practices, failure to train its employees to prevent and detect cyber intrusions, failure to timely and accurately notice them of the Data Breach. Accordingly, Plaintiff brings this Class Action on behalf of herself and all others harmed by Afni's misconduct and seeks damages and

[3] *See* Afni's Notice of Data Breach letter, *accessible at* https://oag.ca.gov/system/files/Afni%20-%20Sample%20Notice.pdf ("Notice")

[4] *See* Afni's regulatory report to the Office of the Maine Attorney General, *accessible at* https://apps.web.maine.gov/online/aeviewer/ME/40/22f470bc-511d-4067-911d-bbf0b230e9c6.shtml

injunctive and other equitable relief.

PARTIES

12. Plaintiff is a natural person and citizen of Illinois, residing in Normal, Illinois, where she intends to remain. Plaintiff is a former Afni employee who received a Notice letter dated June 14, 2022. The Notice letter informed her that over a year ago her PII was involved in the Data Breach.

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

JURISDICTION & VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and at least one member of the putative class if a citizen of a state other than Defendant.

15. This Court has personal jurisdiction over Defendant because it is incorporated under the laws of Illinois and headquartered in this District, and it conducts substantial business in Illinois and this District.

16. Venue is proper in this District because Defendant resides in this District and a substantial part of the events and omissions giving rise to this action occurred in this District.

BACKGROUND FACTS

17. In business since 1930, Afni is a provider of telecommunication, customer assistance, remote management, insurance subrogation, and consumer debt collection services

and employs 9,000 individuals worldwide.[5]

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

19. Afni also collects consumers' PII in the normal course of its business, either directly or indirectly, including their names, addresses, Social Security numbers, and financial account information.

20. Afni's employees and consumers who entrust it with sensitive PII do so based on Afni's promise to keep it confidential and with the mutual understanding that Afni will safeguard the information from theft and misuse.

21. Afni knew, in the course of collecting and Maintaining Plaintiff and Class Members PII that it was a target of cybercriminals seeking that PII and that cyberattacks were a foreseeable threat. Afni also understood the severe consequences that would result to Plaintiff and the Class if it failed to safeguard their data or warn them of any incidents involving their PII.

22. 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.

23. Indeed, Afni's Chief Executive Officer notes "[r]isk management and information

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

security are more critical than ever[.]"6 And its Chief Information Security Officer warns: "[t]he 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."

24. But despite understanding the importance of securing PII, Afni failed to follow industry standard practices in securing PII, adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems.

25. Afni materially misled Plaintiff and Class Members about the extent and scope of its data security practices, by misrepresenting it commitment to securing PII and materially omitting its inadequate data security practices and the existence of the Data Breach itself. Defendant did so prior to and in the twelve months following the Data Breach and did so to divert revenue intended for data security to its own profit and to protect itself from reputational damage and loss of business that may result from public awareness of the Data Breach.

26. As a result, Afni left the PII of Plaintiff and the Class an unguarded target for theft and misuse and Plaintiff and Class Members were harmed.

The Ransomware Attack and Data Breach were Foreseeable Risks of which Defendant was on Notice

27. It is well known that PII, including financial account information in particular, is an invaluable commodity and a frequent target of hackers.

28. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[7]

---

[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).

[7] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf

29. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[8]

30. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[9]

31. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

32. Individuals are particularly concerned with protecting the privacy of their financial account information, which are the "secret sauce" that is "as good as your DNA to hackers."

33. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Afni knew or should have known that its electronic records would be targeted by cybercriminals.

34. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

[8] *Id*.
[9] *Id* at p. 15.

35. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Afni failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

At All Relevant Times Afni Had a Duty to Plaintiff and Class Members to Properly Secure their Private Information

36. At all relevant times, Afni had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to promptly notify Plaintiff and Class Members when Afni became aware that their PII may have been compromised.

37. Afni's duty to use reasonable security measures arose as a result of its voluntary undertaking to collect and maintain the PII of its employees and consumers generally and its failure to use ordinary and reasonable care with respect to its collection and maintenance of that PII.

38. Afni had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Afni breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

39. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

40. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."10 The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."11

41. The ramifications of Afni's failure to keep its Class Members' PII secure are long lasting and severe. Once PII is stolen, particularly financial information, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Personally Identifiable Information

42. PII of data breach victims remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to

[10] 17 C.F.R. § 248.201 (2013).
[11] *Id*.

$200, and bank details have a price range of $50 to $200.12 According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.13

43. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."14

44. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.15

45. Given the nature of Afni's Data Breach, as well as the long delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII may easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

---

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed December 10, 2021).

[13] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed December 10, 2021).

[14] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed December 10, 2021).

[15] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

46. 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.

47. 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.

48. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

49. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

50. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-

[16] *See* U.S. Gov. Accounting Office, GAO-07-737, "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" (GOA, 2007). Available at https://www.gao.gov/new.items/d07737.pdf.

market" for years.

51. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

52. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

53. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, basic credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.17 The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as dates of birth).

54. To date, Afni has only offered its Class Members twelve months of credit monitoring services even with the four-month delay from their discovery of the Data Breach to the production of the notice letters. The advice offered to victims in the notice letters is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

55. The injuries to Plaintiff and Class Members were directly and proximately caused by Afni's failure to implement or maintain adequate data security measures for the Class Members.

[17] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed December 10, 2021).

Defendant failed to adhere to FTC guidelines.

56. 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.

57. 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.

58. 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.

59. 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.

60. 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.

61. 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.

Plaintiff's Experience

62. Plaintiff is a former Afni employee who worked for the company from around April 2018 through around April 2022.

63. As a condition of Plaintiff's employment, Afni required Plaintiff to provide her PII. Plaintiff provided her PII to Afni on the promise and mutual understanding that Afni would use reasonable measures to protect it.

64. Between June 2021, when Afni discovered the Data Breach, and June 2022 when Afni disclosed it, Plaintiff suffered at least seven instances of identity theft.

65. Since July 2021—one month after the Data Breach—Plaintiff has had to replace one of her payment cards five times because her account information has been repeatedly breached.

66. 11 months after the Data Breach, in May 2022, Plaintiff suffered yet another fraudulent charge on one of her financial accounts.

67. A year after the Data Breach, in June 2022, Plaintiff was charged $500 for an online purchase that she did not authorize. Plaintiff was unable to have the full charge refunded and received only $250 back.

68. Plaintiff has also received an uptick in spam texts and phone calls following the breach and has to spend considerable time and endure frustration dealing with these suspicious communications.

69. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from future identity theft and estimates she has spent around 5 hours dealing with the attempts to steal her identity to date.

70. Plaintiff fears for her personal financial security and uncertainty over the PII exposed in the Data Breach and future fraud attempts. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

71. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

72. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

73. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

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

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

75. 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:

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

g. The diminution in value of their PII;

h. The compromise and continuing publication of their PII;

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

j. 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;

k. Delay in receipt of tax refund monies;

l. Unauthorized use of stolen PII; and

m. 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.

CLASS ACTION ALLEGATIONS

76. Plaintiff brings this action on behalf of two classes of similarly persons.

77. The classes of persons Plaintiff proposes to represent are defined, subject to amendment as appropriate, as:

> **The Nationwide Class**: All persons Afni identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").
>
> **The Employee Subclass**: All persons who are current or former Afni employees whose PII was compromised in the Data Breach, including all who were sent a notice of the Data Breach (the "Subclass").

78. Excluded from the Employee Subclass and Nationwide Class (together "Classes") are counsel, Afni, any entities in which Afni has a controlling interest, Afni's agents and

employees, any judge to whom this action is assigned, and any member of such judge's staff and immediate family.

79. Numerosity: Member of the Classes are so numerous that joinder of all members is impracticable. Defendant has identified and sent notice to over 261,000 persons whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

80. Commonality: There are questions of law and fact common to Plaintiff and to the proposed Classes, including but not limited to the following:

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

b. Whether Afni 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. Whether Afni was negligent in maintaining, protecting, and securing PII;

d. Whether Afni breached contract promises to safeguard Plaintiff and the Classes' PII;

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

f. Whether Afni's Breach Notice was reasonable;

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

h. What the proper damages measure is;

i. Whether Afni violated the statutes alleged in this complaint; and

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

81. Defendant engaged in a common course of conduct giving rise to the legal rights Plaintiff seeks to enforce, on behalf of herself and the other members of the Classes, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale in comparison, in both quality and quantity, to the numerous common questions that dominate this action. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

82. Predominance: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

83. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to that of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel

experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

84. Superiority: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large companies, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

85. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

86. Typicality: Plaintiff's claims are typical of those of other Class Members because

Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

87. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

88. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

89. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

90. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive relief with regard to the Class Members as a whole is appropriate..

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

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

92. Defendant owed a duty of care to Plaintiff and Class Members as a result of its voluntary decision to collect and maintain the PII of Plaintiff and the Classes. 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.

93. 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.

94. 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.

95. 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.

96. 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.

97. 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.

98. 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.

99. 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.

100. 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.

101. 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.

102. 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.

103. 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.

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

105. 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.

106. 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
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 Ill. Comp. Stat. §§ 505/1, *et seq*.
(On Behalf of Plaintiff and the Nationwide Class)

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

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

109. Defendant is headquartered in and directs its business from Illinois and the acts and omissions alleged herein, including Defendant's data security practices and policies and its response to the Data Breach were decided in and directed from Illinois.

110. There is a consumer nexus between the claims of Plaintiff and the Class in that Defendant's acts and omissions involve trade practices that are directed to the consumer marketplace and implicate consumer protection concerns for the approximately 260,000 victims of the Data Breach, the vast majority of whom are consumers as defined in 815 Ill. Comp. Stat. § 505/1(e). Defendant collected and maintained the PII of consumers as a necessary and regular part of its business and its failure to safeguard that PII and timely notice victims of the Data Breach injured those consumers and left those consumers vulnerable to future harm. The relief requested herein would provide compensatory and injunctive relief to those consumers and protect them from the imminent threat of future harm arising from the Data Breach.

111. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and

advertisement of their services in violation of the CFA, including: (1) failing to maintain adequate data security to keep Plaintiff's and the Class's sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiff and the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff and the Class; (3) failing to disclose or omitting materials facts to Plaintiff and the Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff and the Class; (4) failing to disclose or omitting material facts concerning the occurrence of the Data Breach and to failing protect Plaintiff and members of the Class by timely noticing them that the Data Breach had occurred twelve months prior; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and the Class's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

112. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Class and defeat their reasonable expectations about the security of their PII.

113. Defendant intended that Plaintiff and the Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

114. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class.

Plaintiff and the Illinois Subclass have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

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

116. As a result of Defendant's wrongful conduct, Plaintiff and the Class were injured in that they never would have entrusted their PII to Defendant, or relied on or accepted Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

117. As a direct and proximate result of Defendants' violations of the CFA, Plaintiff and the Class have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiff and the Class would not have made had they known of Defendants' inadequate data security; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

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

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

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

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

121. In turn, and through internal policies and express and implied promises, Defendant agreed it would not disclose the PII it collects to unauthorized persons and would safeguard employee PII from unauthorized access.

122. Plaintiff and the members of the Employee Subclass accepted Defendant's offer by providing PII to Defendant in exchange for employment with Defendant and with the mutual understanding and intent that Defendant would safeguard the PII.

123. 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.

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

125. 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.

126. 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).

127. 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.

128. 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.

129. 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.

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

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

132. 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 Plaintiff and the Employee Subclass)

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

134. This claim is pleaded in the alternative to the breach of implied contractual duty claim for the Employee Subclass.

135. Plaintiff and members of the Classes conferred a benefit upon Defendant in the form of the provision of their PII and Defendant would be unable to engage in its regular course of business without that PII.

136. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and members of the Classes. Defendant also benefited from the receipt of Plaintiff and members of the Classes' PII, as this was used to facilitate employment and defendant's consumer facing business activities.

137. Defendant was to have used a portion of the revenue it derived from Plaintiff's and the Classes' PII to employ reasonable data security protocols and to safeguard that PII. Instead, Defendant diverted that portion of its revenue to its own profit at the expense of Plaintiff and the Classes.

138. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Classes' PII because Defendant failed to adequately protect their PII. Plaintiff and the Classes would not have provided their or entrusted

their PII or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their PII.

139. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Classes 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 Classes;

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.

RESPECTFULLY SUBMITTED AND DATED this 29th day of August, 2022.

/s/ *Gary M. Klinger*
Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 West Monroe Street, Suite 2100
Chicago, IL 60606
(866) 252-0878
gklinger@milberg.com

Attorneys for Plaintiff