**UNITED STATES DISTRICT COURT**
**NORTHERN DISTRICT OF GEORGIA**
**ATLANTA DIVISION**

| | | |
|---|---|---|
| **OMAR AVILES, individually, and on behalf of all others similarly situated,** | ) | |
| ***Plaintiff*** | ) | |
| **V.** | ) | **Civil Action No._____** |
| **ASBURY AUTOMOTIVE GROUP, INC.** | ) | |
| ***Defendant*** | ) | |

**COMPLAINT—CLASS ACTION**

Plaintiff, Omar Aviles ("Plaintiff" or "Aviles"), individually and on behalf of all others similarly situated, complains and alleges as follows against Defendant, ASBURY AUTOMOTIVE GROUP, INC. ("Defendant" or "Asbury") based on personal knowledge, on the investigation of his counsel, and on information and belief as to all other matters:

## INTRODUCTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from Defendant Asbury, arising from its failure to safeguard certain Personally Identifying Information[1] ("PII") and other sensitive, non-public

[1] The Federal Trade Commission defines "personally identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to

financial information (collectively, "Personal Information") of thousands of its prospective, current, and former employees, resulting in Defendant's network systems being unauthorizedly accessed on or around December 25, 2023, and the Personal Information of employees therein, including of Plaintiff and the proposed Class Members, being disclosed, stolen, compromised, and misused, causing widespread and continuing injury and damages.

2. On information and belief, on or around December 25, 2023, Asbury's file servers were "hacked" and unauthorizedly accessed, resulting in the unauthorized disclosure of the Personal Information of Plaintiff and the Class Members, including names, Social Security Numbers,[2] Driver's license numbers, and state identification numbers (the "Data Breach").[3]

3. As explained below, Plaintiff and Members of the Class have suffered significant injury and damages due to the Data Breach permitted to occur by Asbury, and the resulting misuse of their Personal Information, monetary damages including

---

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." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the breach.

[2] *See:* Asbury Notice of Data Breach to Plaintiff Aviles, April 22, 2024, attached as **Exhibit A**; and
Asbury sample Notice of Data Breach to Maine Attorney General, available at https://apps.web.maine.gov/online/aeviewer/ME/40/0dae7fdc-1086-4708-9e8c-a07294ed1ada.shtml (last accessed May 6, 2024).

[3] *Id.*

out-of-pocket expenses, including those associated with the reasonable mitigation measures they were forced to employ, and other damages. Plaintiff and the Class also now forever face an amplified risk of *further* misuse, fraud, and identity theft due to their sensitive Personal Information falling into the hands of cybercriminals as a result of the tortious conduct of Defendant.

4. On behalf of himself and the Class preliminarily defined below, Plaintiff brings causes of action for negligence, negligence *per se*, breach of express and implied contractual duties, unjust enrichment, and bailment. Plaintiff seeks damages and injunctive and declaratory relief arising from Asbury's failure to adequately protect his highly sensitive Personal Information.

**PARTIES**

5. Plaintiff Aviles is a natural person and citizen of the state of Arizona, residing in Tucson, Arizona, in the County of Pima, where he intends to remain. Plaintiff is a current employee of Asbury.

6. Defendant, Asbury Automotive Group, Inc. is a corporation organized and existing under the laws of the state of Delaware, with a principal place of business located at 2905 Premiere Parkway, Suite 300, Duluth, Georgia, 30097.

7. Asbury is a Fortune 500 Company and "one of the largest automotive

retail and service companies in the U.S."[4] Asbury currently operates over 157 dealerships across 16 states in the U.S.[5] Asbury reported a total annual revenue of $14.8 billion for 2023.[6]

8. Asbury touts itself as "one of America's Greatest Workplaces" according to Newsweek and represents that its "mission is to create an environment where all associates can thrive professionally and personally."[7]

9. Asbury's employees work throughout the United States, in Washington, Idaho, California, Utah, Colorado, Arizona, New Mexico, Texas, Missouri, Indiana, Georgia, South Carolina, Florida, Virginia, Maryland, and Delaware.[8]

10. According to Asbury, "Safeguarding the personal information of our guests, team members, and business partners is central to our efforts around regulatory compliance and a crucial part of building trust with our stakeholders." [9]

11. On information and belief, Asbury failed to undertake adequate measures to safeguard the Personal Information of Plaintiff and the proposed Class Members, including failing to implement industry standards for data security, and

[4] *See*, Asbury Automotive Group Reports Fourth Quarter Financial Results, available at https://investors.asburyauto.com/press-releases/20241 (last accessed May 6, 2024).
[5] *Id.*
[6] *Id.*
[7] *See* https://www.asburyauto.com/careers (last accessed Apr. 30, 2024).
[8] *See* Asbury's Corporate Responsibility Report, 2023 https://online.flippingbook.com/view/751706128/4/ (last accessed May 6, 2024).
[9] *Id.*, p. 36.

failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

12. As a direct and proximate result of Defendant's failures to protect Plaintiff's and the Class Members' sensitive personal information and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class have suffered widespread injury and damages necessitating Plaintiff seeking relief on a class wide basis.

## JURISDICTION AND VENUE

13. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because: (i) there are more than one hundred (100) Class Members; (ii) the aggregate amount in controversy exceeds five million dollars ($5,000,000.00), exclusive of interest and costs; and (iii) some Class Members are citizens of states different than Asbury.

14. This Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business in this State; it maintains its principal place of business and headquarters in Georgia; and committed tortious acts in Georgia.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to these claims occurred in this district, and/or or a substantial part of property that is the subject of this action

is situated herein.

## FACTUAL ALLEGATIONS

### A. Plaintiff and the Class Members entrusted their Personal Information to Asbury

16. Plaintiff Omar Aviles and the Members of the proposed Class are current and former employees and prospective employees of Asbury.

17. From 2013 to present, Plaintiff has been employed by Defendant.

18. As a condition of employment, and/or of applying for employment with Asbury, Plaintiff and the Class Members were required by Asbury to confide and make available to it their sensitive and confidential Personal Information, including, but not limited to, their names and Social Security Numbers, and Driver's License numbers, and/or State Identification Numbers.

19. Asbury maintains records of its employees' information such as their full names, Social Security Numbers, dates of birth, driver's license numbers, and financial account information in the ordinary course of business. These records are stored on Asbury's network systems.

20. In its Privacy Policy, Asbury informs employees that it "takes privacy seriously and is committed to safeguarding your privacy." Asbury states it "takes commercially reasonable physical, electronic, and managerial measures to safeguard and secure any information [provided to Asbury] (e.g. data will be stored in protected databases on secured servers with restricted access.)." The Privacy Policy is

attached hereto as **Exhibit B.**

21. Asbury represented to its employees that their Personal Information would be secure.

22. The Data Breach that is the subject of this civil action is not contemplated or permitted by Asbury's Privacy Policy.

23. Asbury acquired, collected, and stored a massive amount of said Personal Information of its employees, including Mr. Aviles and the Members of the proposed Class, which it stored in its electronic systems.

24. By obtaining, collecting, using, and deriving a benefit from its employees' Personal Information, Asbury assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting their Personal Information from unauthorized disclosure.

25. Plaintiff has taken reasonable steps to maintain the confidentiality of his Personal Information. Plaintiff, as a current employee, relies on Asbury to keep his Personal Information confidential and securely maintained, to use this information for authorized purposes and disclosures only.

26. In its Privacy Policy, Asbury promises that it will not sell Personal Information to third parties for business or commercial purposes, and that it will disclose Personal Information as described in the policy or in any other applicable privacy notices or opt-ins that website visitors may receive; that Asbury will disclose

Personal Information to third parties only with consent; to business partners or agents; for business transfers or assignments; and as required by law.[10]

27. The Data Breach that is the subject of this civil action is not contemplated or permitted by Asbury's website Privacy Policy.

28. Plaintiff and the proposed Class Members entrusted their Personal Information to Asbury solely for the purposes of applying for employment with Defendant and/or as a condition of employment, with the expectation and implied mutual understanding that Asbury would strictly maintain the confidentiality of the information and undertake adequate measures to safeguard it from theft or misuse.

29. Plaintiff and the proposed Class Members would not have entrusted Asbury with their highly sensitive Personal Information if they had known that Asbury would fail to take adequate measures to protect it from unauthorized use or disclosure.

## B. Plaintiff's and the Class Members' Personal Information was Unauthorizedly Disclosed and Compromised in the Data Breach

30. As stated prior, Plaintiff Aviles has been employed by Defendant since May 2013.

31. As a prerequisite to employment, Plaintiff and the Class Members disclosed their non-public and sensitive Personal Information to Asbury, with the

[10] *See id.*

implicit understanding that their Personal Information would be kept confidential. This understanding was based on all the facts and circumstances attendant to their employment there, and the express, specific, written representations made by Asbury and its agents.

32. Plaintiff and the Class Members reasonably relied upon Asbury's representations to their detriment and would not have provided their sensitive Personal Information to Asbury if not for Asbury's explicit and implicit promises to adequately safeguard that information.

33. On or about April 22, 2024, Asbury began sending letters to the Class Members notifying them that their Personal Information had been compromised during the Data Breach ("Notice").[11] Plaintiff Aviles received the Notice during the week of May 4, 2024. *See* Exhibit A.

34. According to Asbury's Notice,

> On December 25, 2023, we detected unauthorized access to files on some of our file servers. Immediately upon identifying the unauthorized activity, we implemented our incident response plan, took steps to contain the activity, and launched an investigation. A cybersecurity firm that has assisted other companies in similar situations was engaged and law enforcement was notified. The investigation identified that an unauthorized actor accessed certain systems in our network and, on December 25, 2023, acquired files stored on some of our file servers.

Ex. A.

[11] *See* Notice of Data Breach, April 22, 2024 (Exhibit A)

35. Defendant further represented that it had implemented additional technical safeguards to enhance the security of information in its possession and prevent similar incidents from happening in the future.[12]

36. Asbury urged those affected by the Data Breach to remain vigilant in regularly reviewing and monitoring their accounts for suspicious activity. Asbury encouraged Plaintiff and the class to immediately contact the Federal Trade Commission or the Attorney General's office if they believe their Personal Information was misused.[13]

37. In addition, Asbury's Notice provided a toll-free telephone number for affected persons receiving the Notice to call for their questions to be addressed.[14]

38. Asbury offered complimentary credit monitoring and identity protection services through Identity Defense.

39. As a result of this Data Breach, the Personal Information of Plaintiff and the proposed Class Members was unauthorizedly disclosed and compromised in the Data Breach.

40. The Data Breach was preventable and a direct result of Asbury's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect employees' Personal Information.

---

[12] *Id.*
[13] *Id.*
[14] *Id.*

41. In addition, while Asbury allegedly discovered the Data Breach on December 25, 2023, as reported to the Maine Attorney General, it is clear from Defendant's Notice that it waited until April 22, 2024, before it began properly notifying the class—a full *four months* after Defendant discovered its Data Breach.[15]

C. **The Data Breach was Foreseeable by Asbury**

42. Plaintiff's and the proposed Class Members' PII was provided to Asbury with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. By failing to do so, Defendant put all Class Members at risk of identity theft, financial fraud, and other harms.

43. Defendant tortiously failed to take the necessary precautions required to safeguard and protect the PII of Plaintiff and the Class Members from unauthorized disclosure. Defendant's actions represent a flagrant disregard of Plaintiff' and the other Class Members' rights.

44. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

[15] Asbury report to Maine Attorney General, available at https://apps.web.maine.gov/online/aeviewer/ME/40/0dae7fdc-1086-4708-9e8c-a07294ed1ada.shtml (last accessed May 6, 2024).

45. Cyber-attacks against companies such as Defendant are targeted and frequent. Indeed, according to UpGuard, "[c]ybercriminals know that tech companies often have weaker data protection and overall cybersecurity measures than highly-regulated industries, like healthcare and finance. Instead of targeting these organizations directly for their valuable data, they focus their efforts on the poor data security often found in the first link of the supply chain – tech vendors that store and manage significant amounts of data from these industries."[16]

46. According to the Identity Theft Resource Center's January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[17]

47. 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 Asbury. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach

[16] UpGuard, Catherine Chipeta, "5 Ways Tech Companies Can Prevent Data Breaches," updated Mar. 2, 2023 available at https://www.upguard.com/blog/how-tech-companies-can-prevent-data-breaches (last accessed May 6, 2024).

[17] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last accessed May 6, 2024).

will happen, but when."[18]

48. Based on data from the Maine Attorney General, as of August 2022, "…at least 79 financial service companies have reported data breaches affecting 1,000 or more consumers, and the total number of consumers affected by these breaches could be as high as 9.4 million."[19]

49. PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web.

50. PII can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. 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.

51. Given the nature of the Data Breach, it was foreseeable that the

[18] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last accessed May 6, 2024).
[19] Carter Pape, "Breach data from Maine shows scope of bank, credit union exposures," American Banker, August 24, 2022, available at https://www.americanbanker.com/news/breach-data-from-maine-shows-scope-of-bank-credit-union-exposures

compromised PII could be used by hackers and cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff' and the Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in the Class Members' names.

## D. Asbury failed to sufficiently protect the Personal Information that Plaintiff and the Proposed Class Members Had Entrusted to It.

### *i. Asbury failed to adhere to FTC guidelines*

52. According to the Federal Trade Commission("FTC"), the need for data security should be factored into all business decision-making.[20] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Asbury, should employ to protect against the unlawful exposure of Personal Information.

53. 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.[21] The guidelines explain that businesses should:

a. protect the personal information that they keep;

[20] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Sep. 2, 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed May 6, 2024).

[21] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Sep. 28, 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

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.

54. 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.

55. The FTC recommends that companies not maintain PII 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.[22]

56. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, 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.

[22] *See Start with Security*, *supra* n.40.

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

***ii. Asbury failed to adhere to industry standards***

58. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

59. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[23]

[23] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last accessed May 6, 2024).

60. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra*, such as:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[24]

61. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cybersecurity attacks, including (1) reducing the likelihood of a damaging cyber intrusion by validating

[24] Federal Trade Commission, "Understanding The NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last accessed May 6, 2024).

that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (2) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (3) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[25]

62. Upon information and belief, Asbury failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both 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,

[25] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last acc. Sept. 26, 2023).

and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiff's and the proposed Class Members' PII, resulting in the Data Breach.

**E. Plaintiff and the Class Members were significantly injured by the Data Breach**

63. Plaintiff and members of the proposed Class have suffered injury and damages from the exfiltration and misuse of their PII that can be directly traced to Asbury, that has occurred, is ongoing, and/or imminently will occur.

64. As stated prior, in the Data Breach, unauthorized cybercriminals were able to access and acquire Plaintiff's and the proposed Class Members' PII, which is now available to be imminently used for fraudulent purposes or has been sold for such purposes, causing widespread injury and damages.

65. The ramifications of Asbury's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

66. Because Asbury failed to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress.

Plaintiff and the Class Members have suffered, will imminently suffer, or are at an increased risk of suffering:

a. Fraudulent misuse of PII;

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

c. The diminution in value of their PII;

d. The compromise and continuing publication of their PII;

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

f. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying 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;

g. Delay in receipt of tax refund monies;

h. Increase in spam texts and telephone calls;

i. Unauthorized use of stolen PII; and

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

67. Furthermore, the Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft.

68. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[26]

69. The FTC recommends that identity theft victims take time and effort intensive or costly steps to protect their personal and financial information after a data breach, including contacting the company where the fraud occurred and asking them to close or freeze accounts and changing login information; contacting one of the credit bureaus to place a fraud alert on credit files (consider an extended fraud

[26] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last accessed May 6, 2024).

alert that lasts for 7 years if someone steals their identity); reviewing their credit reports; seeking a credit freeze; correcting their credit reports; and other steps such as contacting law enforcement and reporting the identity theft to the FTC.[27]

70. Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud—just as occurred here—phone or utilities fraud, and bank/finance fraud.

71. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

72. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive other services in the victim's name, and may even give the victim's PII to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

73. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: For example, nearly 30% of victims have been the victim of a previous identity

[27] *See* Federal Trade Commission, available at https://www.identitytheft.gov/Steps (last accessed May 6, 2024).

crime; an all-time high number of victims say they have contemplated suicide. 35% reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. 54% percent reported feelings of being violated. [28]

74. What's more, theft of PII is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, PII is valuable property.[29]

75. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that PII has considerable market value.

76. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between

[28] Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last accessed May 6, 2024).

[29] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private information") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

when PII and/or financial information is stolen and when it is used.

77. PII are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

78. Where the most PII belonging to Plaintiff and Class Members was accessible from Asbury's network, 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 the Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and the Class Members must vigilantly monitor their financial accounts for many years to come.

79. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[30]

80. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for

[30] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed May 6, 2024).

additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[31] Each of these fraudulent activities is difficult to detect. An individual may not know that his or his Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

81. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[32]

82. 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

[31] *See id.*

[32] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed May 6, 2024).

information and Social Security Numbers are worth more than 10x on the black market."[33] Accordingly, the Data Breach has caused Plaintiff and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the unauthorized disclosure, lost time and efforts in remediating the impact of the Data Breach, and other injury and damages as set forth in the preceding paragraphs.

83. Another example of criminals using PII for profit is the development of "Fullz" packages.[34]

84. 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

[33] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, 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 May 6, 2024).

[34] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/.

individuals. These dossiers are known as Fullz packages.

85. The development of Fullz packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's 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 Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

86. Asbury knew or should have known of these harms which would be caused by the Data Breach it permitted to occur, and strengthened its data systems accordingly.

**F. *Plaintiff Aviles' Experience***

87. Plaintiff Aviles entrusted his PII to Asbury in connection with his employment.

88. Plaintiff Aviles received Asbury's Data Breach Notice on or around May 4, 2024, informing him that his PII was compromised in the Data Breach,

including at least his name and Social Security number.

89. As a direct result of the Data Breach, Plaintiff Aviles has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of his PII that can be directly traced to Defendant.

90. Plaintiff Aviles' PII unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

91. Plaintiff Aviles has spent time mitigating the effects of the Data Breach by researching the Data Breach and reviewing the materials Defendant sent Plaintiff.

92. In addition, Plaintiff Aviles must now spend additional time and effort attempting to remediate the harmful effects of the Data Breach, including monitoring his credit reports, and fears for his personal financial security and uncertainty over the information compromised in the Data Breach. He is experiencing feelings of anxiety, sleep disruption, stress, and fear 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 is contemplated and addressed by law.

93. Plaintiff Aviles was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing his highly sensitive PII and the harm caused by the Data Breach.

94. As a result of Asbury's Data Breach, Plaintiff Aviles faces a lifetime

risk of additional identity theft.

## CLASS ACTION ALLEGATIONS

95. Plaintiff brings this action on behalf of himself and all others similarly situated pursuant to Fed. R. Civ. Proc. 23. The Class is preliminarily defined as:

> All individuals whose Personal Information was compromised as a result of the Data Breach with Asbury which was announced on or about April 24, 2024.

96. Excluded from the Class are Asbury and its subsidiaries and affiliates, officers, directors, and members of their immediate families, and any entity in which it has a controlling interest, the legal representatives, heirs, successors or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

97. Plaintiff reserves the right to modify or amend the definition of the proposed Class and/or to add a subclass(es) if necessary, before this Court determines whether certification is appropriate.

98. *Fed. R. Civ. Proc. 23(a)(1) Numerosity:* The Class is so numerous such that joinder of all Members is impracticable. Upon information and belief, and subject to class discovery, the Class consists of thousands of current and former employees of Asbury, the identity of whom are within the exclusive knowledge of and can be ascertained only by resort to Asbury's records. Asbury has the administrative capability through its computer systems and other records to identify

all Members of the Class, and such specific information is not otherwise available to Plaintiff.

99. *Fed. R. Civ. Proc. 23(a)(2) Commonality and Fed. R. Civ. Proc. 23(b)(3) Predominance:* There are numerous questions of law and fact common to the Class. As such, there is a well-defined community of interest among the Members of the Class. These questions predominate over questions that may affect only individual Members of the Class because Asbury has acted on grounds generally applicable to the Class. Such common legal or factual questions include, but are not limited to:

a. Whether Asbury had a duty to protect employee Personal Information;

b. Whether Asbury knew or should have known of the susceptibility of its systems to a data breach;

c. Whether Asbury's security measures to protect its systems were reasonable considering best practices recommended by data security experts;

d. Whether Asbury was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Asbury's failure to implement adequate data security measures allowed the Data Breach to occur;

f. Whether Asbury's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach, resulting in the unlawful exposure of the Plaintiff's and Class Members' Personal Information;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Asbury's failure to reasonably protect its systems and data network;

h. Whether Plaintiff and Class Members are entitled to relief;

i. Whether Asbury failed to adequately notify Class Members of the compromise of their Personal Information;

j. Whether Asbury assumed a fiduciary duty and/or confidential relationship to Class Members when they entrusted it with their Personal Information;

k. Whether Asbury breached its contracts with Class Members by failing to properly safeguard their Personal Information and by failing to notify them of the Data Breach;

l. Whether Asbury's violation of FTC regulations constitutes evidence of negligence or negligence *per se*;

m. Whether Asbury impliedly warranted to Class Members that the information technology systems were fit for the purpose

intended, namely the safe and secure processing of Personal Information, and whether such warranty was breached.

100. *Fed. R. Civ. Proc. 23(a)(3) Typicality:* Plaintiff's claims are typical of the claims of all Class Members, because all such claims arise from the same set of facts regarding Asbury's failures:

a. to protect Plaintiff's and Class Members' Personal Information;

b. to discover and remediate the security breach of its computer systems more quickly; and

c. to disclose to Plaintiff and Class Members in a complete and timely manner information concerning the security breach and the theft of their Personal Information.

101. *Fed. R. Civ. Proc. 23(a)(4) Adequacy:* Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff is a more than adequate representative of the Class in that Plaintiff is a victim of the Data Breach, has suffered injury and damages such as misuse and fraudulent activity as a result of the Data Breach, and brings the same claims on behalf of himself and the putative Class. Plaintiff has no interests antagonistic to that of the Class Members. Plaintiff has retained counsel who are competent and experienced in litigating class actions, including class actions following data breaches and unauthorized data disclosures. Plaintiff intends to vigorously prosecute this case and will fairly and adequately

protect the Class's interests.

102. *Fed. R. Civ. Proc. 23(b)(2) Injunctive and Declaratory Relief:* Asbury has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

103. *Fed. R. Civ. Proc. 23(b)(3) Superiority:* It is impracticable to bring Class Members' individual claims before the Court. Class treatment permits many similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

104. A class action is superior to the other available methods for the fair and efficient adjudication of this controversy because:

a. The unnamed Members of the Class are unlikely to have an interest in individually controlling the prosecution of separate actions;

b. Concentrating the litigation of the claims in one forum is

desirable;

c. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

d. Plaintiff's legal counsel has the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

105. Plaintiff knows of no unique difficulty to be encountered in the prosecution of this action that would preclude its maintenance as a class action.

106. *Fed. R. Civ. Proc. 23(c)(4) Issue Certification:* Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Asbury owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing and safeguarding their Personal Information;

b. Whether Asbury's security measures to protect its data systems were reasonable considering best practices recommended by data security experts;

c. Whether Asbury's failure to institute adequate protective security

measures amounted to negligence;

d. Whether Asbury failed to take commercially reasonable steps to safeguard prospective employee and employee Personal Information; and

e. Whether adherence to FTC data security recommendations, and industry standards on data security would have reasonably prevented the Data Breach.

107. Finally, all Members of the proposed Class are readily ascertainable. Asbury has access to employee and applicant names and addresses affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing constitutionally sufficient notice.

**COUNT I**
**NEGLIGENCE**

108. Plaintiff Aviles and the Members of the Class incorporate the above allegations as if fully set forth herein.

109. Defendant Asbury owed a duty to Plaintiff and the Members of the Class to exercise reasonable care to safeguard their Personal Information in its possession, based on the foreseeable risk of a data breach and the resulting exposure of their information, as well as on account of the special relationship between Defendant and its employees, 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.

110. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Members of the Class's Personal Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the manner in which the information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

111. Further, Defendant owed to Plaintiff and Members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their Personal Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and Members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and Members of the Class to take appropriate measures to protect their Personal Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

112. Asbury owed these duties to Plaintiff and Members of the Class because they are Members of a well-defined, foreseeable, and probable class of individuals who Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Members of the Class's personal information and PII for employment

purposes.

113. Plaintiff and Members of the Class were required to provide their Personal Information to Defendant as a condition of applying for employment and/or as a condition of employment, and Defendant retained that information.

114. The risk that unauthorized persons would attempt to gain access to the Personal Information and misuse it was foreseeable. Given that Defendant holds vast amounts of this information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Personal Information, whether by hacking attack, or otherwise.

115. Personal Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Personal Information of Plaintiff and Members of the Class, and the importance of exercising reasonable care in handling it.

116. Defendant Asbury breached its duties by failing to exercise reasonable care in supervising its employees and agents, and in handling and securing the Personal Information and PII of Plaintiff and Members of the Class which actually and proximately caused the Data Breach and Plaintiff's and Members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's

and Members of the Class's injuries-in-fact.

117. As a direct, proximate, and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Members of the Class have suffered or will suffer injury and damages, including misuse and fraudulent activity, monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

118. Defendant's breach of its common law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and Members of the Class's 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*

119. Plaintiff and the Class Members incorporate the above allegations as if fully set forth herein.

120. 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's and the Class Members' Personal Information, PII.

121. 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 customers or, in this case, employees' and prospective employees' PII.

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

123. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' and prospective employees' 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 required and solicited, collected, and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to employees in the event of a breach, which ultimately came to pass.

124. The harm that has occurred in the Data Breach is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result 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 the Class Members.

125. Defendant had a duty to Plaintiff and the Class Members to implement and maintain reasonable security procedures and practices to safeguard their PII.

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

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

128. But-for Asbury's wrongful and negligent breach of its duties owed to Plaintiff and the Class, Plaintiff and the Members of the Class would not have been injured.

129. The injury and harm suffered by Plaintiff and the Class Members were the reasonably foreseeable result of Defendant's breach of its 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 Class to suffer the foreseeable harms associated with the exposure of their PII.

130. Had Plaintiff and Members of the Class known that Defendant did not adequately protect employees' and prospective employees' PII, Plaintiff and Members of the Class would not have entrusted Defendant with their PII.

131. As a direct and proximate result of Defendant's negligence *per se*,

Plaintiff and the Class Members have suffered harm, injury, and damages as set forth in the preceding paragraphs.

**COUNT III**
**BREACH OF EXPRESS/IMPLIED CONTRACTUAL DUTY**

132. Plaintiff and Members of the Class incorporate the above allegations as if fully set forth herein.

133. Defendant offered to provide employment to Plaintiff and Members of the Class in exchange for payment.

134. Asbury also required Plaintiff and the Members of the Class to provide Defendant with their Personal Information as a condition of applying for employment, and for employees as a condition of receiving renumeration for labor rendered.

135. In turn, and through its Privacy Policy, Defendant agreed it would not disclose Personal Information it collects to unauthorized persons. Defendant also promised to maintain safeguards to protect their Personal Information.

136. Plaintiff and the Members of the Class accepted Defendant's offer by providing Personal Information to Asbury, in applying for employment, and providing labor to Defendant and receiving renumeration.

137. The agreement was supported by adequate consideration, as it was an exchange of labor for money.

138. Implicit in the Parties' agreement was that Defendant would provide

Plaintiff and Members of the Class with prompt and adequate notice of any and all unauthorized access and/or theft of their Personal Information.

139. Plaintiff and the Members of the Class would not have entrusted their Personal Information to Defendant in the absence of such agreement with Defendant.

140. Asbury materially breached the contract(s) it had entered with Plaintiff and Members of the Class by failing to safeguard such Personal 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 Class by:

a. Failing to properly safeguard and protect Plaintiff' and Members of the Class's Personal Information;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic Personal Information that Defendant received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1).

141. The damages sustained by Plaintiff and Members of the Class as set forth in the preceding paragraphs were the direct and proximate result of Defendant's material breaches of its agreement(s).

142. Plaintiff and Members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

143. The covenant of good faith and fair dealing is implied into every contract. 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.

144. 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.

145. Defendant failed to advise Plaintiff and Members of the Class of the Data Breach promptly and sufficiently.

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

147. Plaintiff and Members of the Class have sustained damages as a result 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**

148. Plaintiff and Members of the Classes incorporate the above allegations as if fully set forth herein.

149. This claim is pleaded in the alternative to the breach of express/implied contractual duty claim.

150. Plaintiff and Members of the Classes conferred a benefit upon Defendant in the form of labor rendered in exchange for renumeration.

151. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and Members of the Class. Defendant also benefited from the receipt of Plaintiff's and Members of the Class's Personal Information, as this was required to facilitate the employment relationship and renumeration, as well as for the purpose of applying for employment.

152. As a result of Defendant's conduct, Plaintiff and Members of the Class suffered actual damages in an amount equal to the difference in value between the value of their labor with reasonable data privacy and security practices and procedures that Plaintiff and Members of the Classes were entitled to, and that labor without unreasonable data privacy and security practices and procedures that they received.

153. Under principals of equity and good conscience, Defendant should not be permitted to retain the monetary value of the labor belonging to Plaintiff and

Members of the Classes because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself for which Plaintiff and Members of the Classes expended labor and that were otherwise mandated by federal, state, and local laws and industry standards.

154. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

**COUNT V**
**BAILMENT**

155. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

156. Plaintiff, the Class Members, and Defendant contemplated a mutual benefit bailment when the Plaintiff and putative members of the Class transmitted their PII to Defendant solely for the purpose of obtaining employment.

157. Plaintiff and the Class entrusted their PII to Defendant for a specific purpose—to obtain employment—with an implied contract that the trust was to be faithfully executed, and the PII was to be accounted for when the special purpose was accomplished.

158. Defendant accepted the Plaintiff's and the Class's PII for the specific purpose of providing employment.

159. Defendant was duty bound under the law to exercise ordinary care and

diligence in safeguarding Plaintiff's and the Class's PII.

160. Plaintiff and the Class's PII was used for a different purpose than the Plaintiff and the Class intended, for a longer time period and/or in a different manner or place than Plaintiff and the Class intended.

161. As set forth in the preceding paragraphs, Plaintiff and the Class Members were damaged thereby.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff, OMAR AVILES, individually and on behalf of all others similarly situated, the Class as heretofore identified, respectfully prays this Honorable Court for judgment as follows:

A. Certification for this matter to proceed as a class action on behalf of the proposed Class under Fed. R. Civ. Proc. 23;

B. Designation of Plaintiff as Class Representatives and designation of the undersigned as Class Counsel;

C. Actual damages in an amount according to proof;

D. Injunctive or declaratory relief;

E. Pre- and post-judgment interest at the maximum rate permitted by applicable law;

F. Costs and disbursements assessed by Plaintiff in connection with this action, including reasonable attorneys' fees pursuant to applicable

law;

G. For attorneys' fees under the common fund doctrine and all other applicable law; and

H. Such other relief as this Court deems just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff, on behalf of himself and the Class, hereby demand a trial by jury pursuant to Fed. R. Civ. Proc. 38(b) on all claims so triable.

Dated: May 7, 2024

Respectfully submitted,

*/s/ Joseph B. Alonso*
Joseph B. Alonso
Georgia Bar No. 013627
Daniel H. Wirth
Georgia Bar No: 873443
**ALONSO & WIRTH**
1708 Peachtree Street, NW
Suite 207
Atlanta, GA 30309
Tel: (678) 928-4472
jalonso@alonsowirth.com
dwirth@alonsowirth.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com

raina@straussborrelli.com

*motion for admission pursuant to Fed. R. Civ. Proc. 89(b) to be made

*Counsel for Plaintiff and the Proposed Class*

# ClassAction.org



---