THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF MISSISSIPPI
WESTERN DIVISION

ANDREA TURNER, on behalf of herself and all others similarly situated, Plaintiffs, v. SWEETWATER FRANCHISE GROUP, LLC and ALFORD, HOLLOWAY, & SMITH, PLLC, Defendants.	Case No.: 5:23-cv-74-DCB-BWR **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Andrea Turner ("Plaintiff") brings this Class Action Complaint against Sweetwater Franchise Group, LLC ("Sweetwater") and Alford, Holloway, & Smith, PLLC ("AHS") (collectively, "Defendants"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard personal identifiable information ("PII")[1] for current and former employees of Sweetwater, including, but not limited to, name and Social Security Number.

2. Sweetwater operates approximately thirty (30) Sonic drive-in restaurants, including twelve (12) locations in Florida; seventeen (17) locations in Mississippi; and one (1) location in

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

Texas.

3. AHS is a certified public accounting firm that assists Sweetwater with its financial and accounting needs.

4. Plaintiff worked at Sweetwater's Sonic drive-in restaurant in Wauchula, Florida; her employment ended approximately a decade before the events described below.

5. Prior to and through February 23, 2023, Sweetwater obtained the PII of Plaintiff and Class Members, including the PII of Plaintiff, and shared that PII, unencrypted, with AHS, which stored that PII, unencrypted, in an Internet-accessible environment on AHS's network.

6. On or before February 23, 2023, AHS learned that an unauthorized external party gained remote access to its network and acquired copies of some files stored on its network, including the PII of Plaintiff and Class Members that AHS obtained from Sweetwater (the "Data Breach").

7. On or around July 17, 2023, AHS began notifying Plaintiff and Class Members of the Data Breach.

8. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. AHS admits that the unencrypted PII obtained by an unauthorized external party included name and Social Security number.

9. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive

information.

10. The PII was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members. Defendants have also purposefully maintained secret the specific vulnerabilities and root causes of the breach and have not informed Plaintiff and Class Members of that information.

11. As a result of this delayed response, Plaintiff and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

12. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

13. Plaintiff and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures

so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

14. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

15. Plaintiff Andrea Turner is a citizen of Florida residing in Zolfo Springs, Florida.

16. Sweetwater is a Texas limited liability company with its principal place of business in Tylertown, Mississippi.

17. AHS is a Mississippi limited liability company with its principal place of business in McComb, Mississippi.

18. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

19. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

20. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member, including Plaintiffs, is a citizen of a state different from OSC to establish minimal diversity.

21. Under 28 U.S.C. § 1332(d)(10), Sweetwater is a citizen of Texas and Mississippi because it is a Texas limited liability company and its principal place of business is in Tylertown, Mississippi.

22. Under 28 U.S.C. § 1332(d)(10), AHS is a citizen of Mississippi because it is a Mississippi limited liability company and its principal place of business is in McComb, Mississippi.

23. The Southern District of Mississippi has personal jurisdiction over Sweetwater because it conducts substantial business in Mississippi and this District.

24. The Southern District of Mississippi has personal jurisdiction over AHS because it conducts substantial business in Mississippi and this District.

25. Venue is proper in this District under 28 U.S.C. §1391(b) because Sweetwater operates in this District, Sweetwater provided and entrusted Plaintiff's and Class Members' PII to AHS in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

26. Plaintiff and Class Members, who are current and former employees of Sweetwater,

provided and entrusted Sweetwater with sensitive and confidential information, including name and Social Security number.

27. Plaintiff and Class Members relied on Sweetwater to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

28. Defendants had duties to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

The Data Breach

29. On or about July 17, 20230, AHS sent Plaintiff a notice of an incident that may have involved her personal information (the "Notice of Data Breach"). AHS informed Plaintiff (and other Class Members in substantially the same form) that:

> Alford, Holloway, & Smith, PLLC ("AHS" or "we") assists Sonic of Wauchula with its accounting and financial needs and in the course of this work we acquired some of your personal information. AHS respects the confidentiality of the information entrusted to us and the privacy of individuals whose personal information we maintain but unfortunately, we are writing to advise you of an incident that may have involved some of your personal information. At this time, we have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft. Nonetheless, because your information was involved in the incident, we are notifying you of the incident and including information about steps you can take to protect yourself against identity theft and fraud, should you feel it is appropriate to do so.
>
> **What Happened.** On February 23, 2023, we learned that an unauthorized third party gained access to our computer network. Upon discovering the incident, we promptly began an internal investigation and engaged a leading computer forensics firm to further examine our network and confirm the security of our systems. As a result of that investigation, we learned that the unauthorized party acquired copies of some files stored on our

systems.

What Information Was Involved? On April 24, 2023, a review of the information in those files determined that they contained your name, together with your Social Security number.

30. AHS admitted in the Notice of Data Breach that an unauthorized actor obtained sensitive information about Plaintiff and Class Members, including name and Social Security number.

31. In response to the Data Breach, AHS claims "we are taking steps to reduce the risk of this type of incident occurring in the future, including implementing additional technical controls." However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

32. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

33. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII for current and former employees who worked at one of Sweetwater's Sonic locations in the decade prior to the Data Breach.

34. Because Defendants had duties to protect Plaintiffs' and Class Members' PII, Defendants should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

35. In the years immediately preceding the Data Breach, Defendants knew or should have known that AHS's computer systems were a target for cybersecurity attacks, including attacks involving data theft, because warnings were readily available and accessible via the internet.

36. In light of the information readily available and accessible on the internet before the Data Breach, Sweetwater, having elected to share the unencrypted PII of its current and former employees with AHS, and AHS, having elected to store that PII in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendants' types of businesses had cause to be particularly on guard against such an attack.

37. Prior to the Data Breach, Defendants knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

38. Prior to the Data Breach, Defendants knew or should have known that they should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Sweetwater Acquires and Shares with AHS the PII of Plaintiff and Class Members.

39. As a condition of being a past or current employees at one of Sweetwater's Sonic locations, Sweetwater required that Plaintiff and Class Members entrust Sweetwater with highly confidential PII.

40. Sweetwater shared the PII of Plaintiff and Class Members with AHS, which stored the PII on its Internet-accessible network.

41. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that they were

responsible for protecting the PII from disclosure.

42. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

43. Defendants could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members. Alternatively, Defendants could have destroyed the data they no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

44. Defendants' negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

45. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

46. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[2] 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,

[2] 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number."[3]

47. The ramifications of Defendants' failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

48. The PII of individuals 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 $200, and bank details have a price range of $50 to $200.[4] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[5] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[6]

49. Social Security numbers, for example, are among the worst kind of personal information 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:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use

---

[3] *Id*.

[4] *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 Jan. 26, 2022).

[5] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2022).

[6] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 29, 2020).

> your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[7]

50. What is more, it is no 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. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

51. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The 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."[8]

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

53. This data demands a much higher price on the black market. Martin Walter, senior

---

[7] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 26, 2022).

[8] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 26, 2022).

director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[9]

54. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

55. The fraudulent activity resulting from the Data Breach may not come to light for years.

56. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), 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.[10]

57. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if AHS's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

---

[9] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 26, 2022).

[10] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Mar. 15, 2021).

58. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

59. Defendants were, or should have been, fully aware of the unique type and the significant volume of data contained in the PII that Sweetwater shared with AHS, amounting to potentially thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

60. To date, AHS has offered Plaintiff and Class Members only one year of identity protection services through Experian. The offered service 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.

61. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff's Experience

62. Approximately a decade before the Data Breach, Plaintiff worked at Sweetwater's Sonic location in Wauchula, Florida. As a condition of employment, Sweetwater required that she provide and entrust her PII.

63. Plaintiff received AHS's Notice of Data Breach, dated July 17, 2023, on or about that date. The notice stated that Plaintiff's name and Social Security number were accessed by an unauthorized external party.

64. As a result of the Data Breach, Plaintiff's sensitive information was accessed by an unauthorized external party. The confidentiality of Plaintiff's sensitive information has been

irreparably harmed. For the rest of her life, Plaintiff will have to worry about when and how her sensitive information may be shared or used to her detriment.

65. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

66. Additionally, Plaintiff is very careful about sharing her sensitive PII. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

67. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

68. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

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

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

V. CLASS ALLEGATIONS

71. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

72. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose PII was actually or potentially compromised in the data breach that is the subject of the notice sent to Plaintiff and Class Members on or around July 17, 2023 (the "Nationwide Class").

73. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

74. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

75. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Plaintiff last worked at a Sweetwater Sonic location approximately a decade before the Data Breach. If Plaintiff's PII was aggregated with data of other current and former employees at the Sonic location where Plaintiff worked as well as with the PII of employees at other Sonic locations that Sweetwater operates, the compromised dataset would likely include PII for hundreds or thousands of current and former employees.

76. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had duties to protect the PII of Plaintiff and Class Members;

b. Whether Defendants had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiff and Class Members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the

imminent and currently ongoing harm faced as a result of the Data Breach.

77. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

78. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have 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 Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

79. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

80. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): 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 corporations, like Defendants. 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.

81. 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 Defendants 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 Plaintiffs were 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.

82. The litigation of the claims brought herein is manageable. Defendants' 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.

83. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

84. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper

notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

85. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

86. 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 particular issues include, but are not limited to:

a. Whether Defendants owed legal duties to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duties to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Sweetwater on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Sweetwater breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information

compromised in the Data Breach;

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

87. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

88. As a condition of being employees at Sweetwater's Sonic locations, Plaintiff and the Nationwide Class were obligated to provide and entrust Defendants with certain PII.

89. Plaintiff and the Nationwide Class provided and entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and not disclose their PII to unauthorized third parties.

90. Defendants haved full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

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

92. Defendants had duties to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. These duties include, among other things, designing, maintaining, and testing

Defendants' security protocols to ensure that the PII of Plaintiff and the Nationwide Class in Defendants' possession was adequately secured and protected.

93. Defendants also had duties to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII they were no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

94. Defendants also had duties to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Nationwide Class.

95. Defendants' duties to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Sweetwater with their confidential PII, a necessary part of obtaining employment at Sweetwater's Sonic locations, and Sweetwater shared that PII with AHS.

96. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Nationwide Class.

97. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

98. Plaintiff and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored in an Internet-accessible environment.

99. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and the Nationwide Class. Defendants' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Nationwide Class, including basic encryption techniques freely available to Defendants.

100. Plaintiff and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

101. Defendants were in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

102. Defendants had and continue to have duties to adequately disclose that the PII of Plaintiff and the Nationwide Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

103. Defendants had duties to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Nationwide Class.

104. Defendants have admitted that the PII of Plaintiff and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

105. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Nationwide Class during

the time the PII was within Defendants' possession or control.

106. Defendants improperly and inadequately safeguarded the PII of Plaintiff and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

107. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Nationwide Class in the face of increased risk of theft.

108. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

109. Defendants breached their duties to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII they were no longer required to retain pursuant to regulations and which Defendants had no reasonable need to maintain in an Internet-accessible environment.

110. Defendants, through their actions and/or omissions, unlawfully breached their duties to adequately and timely disclose to Plaintiff and the Nationwide Class the existence and scope of the Data Breach.

111. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Nationwide Class would not have been compromised.

112. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the

Nationwide Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

113. As a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Nationwide Class.

114. As a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

115. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

116. As a direct and proximate result of Defendants' negligence, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(Against Sweetwater on Behalf of Plaintiff and the Nationwide Class)

117. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

118. In being employees at Sweetwater's Sonic locations, Plaintiff and the Nationwide Class provided and entrusted their PII to Sweetwater.

119. Sweetwater's Sonic locations required Plaintiff and the Nationwide Class to provide and entrust their PII as condition of being past and current employees.

120. As a condition of being past and current employees at Sweetwater's Sonic locations, Plaintiff and the Nationwide Class provided and entrusted their PII. In so doing, Plaintiff and the Nationwide Class entered into implied contracts with Sweetwater by which Sweetwater agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiff and the Nationwide Class if their PII had been compromised or stolen.

121. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Sweetwater.

122. Sweetwater breached the implied contracts it made with Plaintiff and the Nationwide Class by (i) failing to encrypt Plaintiffs' and the Nationwide Class's PII before sharing it with AHS and (ii) failing to ensure that AHS encrypted the PII while storing it in an Internet-accessible environment, and (iii) failing to ensure that AHS deleted any PII once it no longer had a reasonable need to maintain it in an Internet-accessible environment, and (iv) failing to ensure that AHS otherwise safeguarded and protected the PII.

123. As a direct and proximate result of Sweetwater's above-described breach of implied contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their sensitive information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

124. As a direct and proximate result of Sweetwater's above-described breach of implied contract, Plaintiff and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Declaratory Judgment
(As to Sweetwater on Behalf of Plaintiff and the Nationwide Class)

125. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

126. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

127. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Nationwide Class's PII and whether Sweetwater is currently maintaining data security measures adequate to protect Plaintiff and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs allege that Sweetwater's data security measures remain inadequate. Sweetwater publicly denies these allegations. Furthermore, Plaintiff and the Nationwide Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Sweetwater has undertaken in response to the Data Breach.

128. Plaintiff and the Nationwide Class have an ongoing, actionable dispute arising out of Sweetwater's inadequate security measures, including (i) Sweetwater's failure to encrypt Plaintiffs' and the Nationwide Class's PII before sharing it with OSC, (ii) Sweetwater's failure to ensure that AHS encrypted the PII while storing it in an Internet-accessible environment, (iii) Sweetwater's failure to ensure that AHS deleted any PII it no longer had a reasonable need to maintain in an Internet-accessible environment, and (iv) Sweetwater's failure to ensure that OSC otherwise safeguarded and protected the PII.

129. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Sweetwater owes a legal duty to secure the PII of past and current employees of Sweetwater;

b. Sweetwater continues to breach this legal duty by failing to employ reasonable measures to secure the PII; and

c. Sweetwater's ongoing breaches of its legal duties continue to cause harm to Plaintiff and the Nationwide Class.

130. This Court also should issue corresponding prospective injunctive relief requiring Sweetwater to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Sweetwater to:

a. Encrypt the PII of current and former employees before sharing it with other entities;

b. Ensure that such entities safeguard and protect such PII, including by storing it in encrypted form; and

c. Ensure that such entities delete any such PII they no longer have a reasonable need to maintain.

131. If an injunction is not issued, Plaintiff and the Nationwide Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at AHS or some other entity with which Sweetwater shares the PII. The risk of another such breach is real, immediate, and substantial. If another breach at AHS or another entity with which Sweetwater shares the PII occurs, Plaintiff and the Nationwide Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

132. The hardship to Plaintiff and the Nationwide Class if an injunction is not issued exceeds the hardship to Sweetwater if an injunction is issued. Plaintiff and the Nationwide Class

will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Sweetwater of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Sweetwater has a pre-existing legal obligation to employ such measures.

133. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing or mitigating another data breach at OSC or another entity with which Sweetwater shares the PII, thus eliminating or mitigating the additional injuries that would result to Plaintiff and the Nationwide Class and others whose confidential information would be further compromised.

COUNT IV
Declaratory Judgment
(As to AHS on Behalf of Plaintiff and the Nationwide Class)

134. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 86.

135. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

136. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Nationwide Class's PII and whether AHS is currently maintaining data security measures adequate to protect Plaintiff and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs allege that AHS's data security measures remain inadequate. AHS publicly denies these allegations. Furthermore, Plaintiff and the Nationwide Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further

compromises of their PII will occur in the future. It is unknown what specific measures and changes AHS has undertaken in response to the Data Breach.

137. Plaintiff and the Nationwide Class have an ongoing, actionable dispute arising out of AHS's inadequate security measures, including (i) AHS's failure to encrypt Plaintiffs' and the Nationwide Class's PII while storing it in an Internet-accessible environment, (ii) AHS's failure otherwise safeguard and protect the PII, (iii) AHS's failure to delete any PII it no longer had a reasonable need to maintain.

138. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. AHS owes a legal duty to secure the PII of current and former employees of Sweetwater;

b. AHS continues to breach this legal duty by failing to employ reasonable measures to secure the PII; and

c. AHS's ongoing breaches of its legal duties continue to cause harm to Plaintiff and the Nationwide Class.

139. This Court also should issue corresponding prospective injunctive relief requiring AHS to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct AHS to:

a. Encrypt the PII of Sweetwater's current and former employees;

b. Otherwise safeguard and protect such PII; and

c. Delete any such PII it no longer has a reasonable need to maintain.

140. If an injunction is not issued, Plaintiff and the Nationwide Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at AHS. The risk of another such breach is real, immediate, and substantial. If another breach at AHS occurs, Plaintiff and the Nationwide Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

141. The hardship to Plaintiff and the Nationwide Class if an injunction is not issued exceeds the hardship to AHS if an injunction is issued. Plaintiff and the Nationwide Class will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to AHS of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and OSC has a pre-existing legal obligation to employ such measures.

142. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing or mitigating another data breach at AHS, thus eliminating or mitigating the additional injuries that would result to Plaintiff and the Nationwide Class and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and her Counsel to represent such Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of

Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly

correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of OSC network is compromised, hackers cannot gain access to other portions of OSC's systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees

compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor OSC's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from OSC's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: August 9, 2023

Respectfully Submitted,

/s/ Bradley S. Kelly
Bradley S. Kelly, Esq. (MSB# 101243)
MORGAN & MORGAN, PLLC
4450 Old Canton Road, Suite 200
Jackson, Mississippi 39211
(601) 718-0946
bkelly@ForThePeople.com

Patrick A. Barthle*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
pbarthle@ForThePeople.com

Ryan D. Maxey*
MAXEY LAW FIRM, P.A.
107 N. 11th St. #402
Tampa, Florida 33602
(813) 448-1125
ryan@maxeyfirm.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice applications pending*

ClassAction.org
