UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

STEPHANIE BOOKER, on behalf of herself and all others similarly situated, *Plaintiff*, v. KAPLAN NORTH AMERICA, LLC, *Defendant*.	No. **COMPLAINT – Class Action** JURY TRIAL DEMANDED

Plaintiff Stephanie Booker, on behalf of herself and on behalf of all others similarly situated, alleges the following against Defendant Kaplan North America, LLC ("Kaplan" or "Defendant") upon personal knowledge as to her own acts, and based upon her investigation, her counsel's investigation, and information and belief as to all other matters.

INTRODUCTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant (the "Data Breach"), which held in its possession certain personally identifiable information ("PII") of Plaintiff and Class Members.

2. Defendant Kaplan North America, LLC is an educational services provider that offers test preparation, professional licensure, corporate training and advising, and language training.[1]

[1] *About Kaplan*, KAPLAN NORTH AMERICA, https://kaplan.com/about (last visited April 1, 2026).

3. Defendant owes Plaintiff and Class Members an affirmative duty to adequately protect and safeguard this private information against theft and misuse. Despite such duties created by statute, regulation, and common law, at all relevant times, Defendant utilized deficient data security practices, thereby allowing sensitive and private data to fall into the hands of strangers.

4. Between October 30, 2025, and November 18, 2025, "an unauthorized actor accessed [Kaplan's] computer servers . . . and took certain files."[2]

5. These files contained affected individuals' "name[s], Social Security number[s], and/or driver's license number[s]."[3]

6. Defendant began notifying affected individuals such as Plaintiff on or around March 17, 2026.[4]

7. But for Defendant's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect PII, the Data Breach would not have occurred.

8. Defendant is well aware that it is at high risk of attempted cyberattack due to the high value of the sensitive data.

9. Despite Defendant's awareness of both the value and sensitivity of the data it safeguarded and serious risk presented by insufficient security practices, Defendant did not take sufficient steps to ensure that its systems were secure. Defendant knew or should have known about the risk to the data it stored and processed, and the critical importance of adequate security measures in the face of increasing threats.

10. The Data Breach was directly and proximately caused by Defendant's failure to

[2] *See* Exhibit A.

[3] *Id.*

[4] *Id.*

implement reasonable and industry-standard data security practices necessary to protect its systems from a foreseeable and preventable cyberattack. Through this wrongful conduct, the sensitive PII of Plaintiff and Class Members is now in the hands of cybercriminals, who target this sensitive data for its value to identity thieves. Plaintiff and Class Members are now at a significantly increased and impending risk of fraud, identity theft, and similar forms of criminal mischief—risks which may last the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes. Moreover, Plaintiff and Class Members have lost the inherent value of their private data.

11. By aggregating information obtained from the Data Breach with other sources or other methods, criminals can assemble a full dossier of private information on an individual to facilitate a wide variety of frauds, thefts, and scams.

12. Defendant's failure to notify Plaintiff and Class Members that it had been impacted by the Data Breach for nearly five months after it first began harmed Plaintiff and made it more difficult for Plaintiff to take swift action to respond to the breach.

13. Plaintiff and Class Members have been harmed because they are at immediate risk of having their personal information used against them. Indeed, they have been at risk well before Defendant even notified Plaintiff of the Data Breach. Plaintiff does not know if her data has been sold, transferred, replicated, or irrevocably disseminated and exposed. She suffered harm in the loss of the value of her data which cannot be easily recovered, if ever.

14. Plaintiff, individually and on behalf of a nationwide class, alleges claims of (1) Negligence, (2) Negligence *Per Se*, (3) Breach of Implied Contract, and (4) Unjust Enrichment. Plaintiff also seeks declaratory and injunctive relief. Plaintiff asks the Court to compel Defendant

to adopt reasonable information security practices to secure the sensitive PII that Defendant collects and stores in its databases and to grant such other relief as the Court deems just and proper.

PARTIES

Plaintiff

15. Plaintiff Stephanie Booker is and at all times mentioned herein a resident and citizen of Savannah, Georgia.

Defendant

16. Defendant Kaplan North America, LLC is a Delaware limited liability company with its principal place of business at 1515 West Cypress Creek Road, Fort Lauderdale, FL 33309.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

18. This Court has personal jurisdiction over Defendant through its business operations in this District, including the conduct giving rise to this Action. Defendant's principal place of business is in this District. Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) and 28 U.S.C. § 1391(d) because a substantial part of the events giving rise to this action occurred in this District. Defendant is also based in this District, maintains Plaintiff's and Class Members' PII in this District, and has caused harm to Plaintiff and Class Members from or within this District.

FACTUAL ALLEGATIONS

I. Background

20. Defendant Kaplan North America, LLC was founded as the "first test preparation business in the U.S."[5]

21. Defendant is an educational services provider that offers test preparation, professional licensure, corporate training and advising, and language training.[6]

22. Defendant "is owned by Graham Holdings, which reported $4.9 billion in revenue last year."[7]

23. Defendant now serves over "one million students and thousands of clients and university partners."[8]

24. Defendant's Privacy Center states, "We work hard to safeguard your personal information while delivering products, services, and experiences that you have come to expect from a trusted, global education and operations support services company."[9]

25. Defendant's Privacy Policy states that it collects customer records such as Social Security number, driver's license or state identification card number, financial information, and other sensitive data.[10] Defendant claims to "delete Social Security numbers (except for the last

---

[5] *About Kaplan*, KAPLAN NORTH AMERICA, https://kaplan.com/about (last visited April 1, 2026).

[6] *Id.*

[7] Jonathan Greig, *Education company Kaplan reports data breach impacting more than 230,000*, THE RECORD (MAR. 23, 2026), https://therecord.media/kaplan-data-breach-hack-notification (last visited April 1, 2026).

[8] *Id.*

[9] *Kaplan Privacy Center*, KAPLAN NORTH AMERICA, https://kaplan.com/privacy (last visited April 1, 2026).

[10] *Privacy Policy*, KAPLAN NORTH AMERICA, https://kaplan.com/privacy-policy (last visited April 1, 2026).

four digits) on a monthly basis after the state's reporting requirements have been met and only if the state regulations permit such deletion."[11]

26. Defendant's Privacy Policy also claims that Defendant has "put in place appropriate security measures to prevent your personal information from being accidentally lost, destroyed, used or accessed in an unauthorized way, altered, or disclosed" and "will only retain your information for as long as necessary to fulfill the purposes we collected it for, including to satisfy any legal, accounting, or reporting requirements."[12]

27. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

28. As a result of collecting and storing the PII of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and Class Members' PII from disclosure to third parties.

II. The Data Breach

29. "[A]n unauthorized actor accessed [Defendant's] computer servers between October 30, 2025, and November 18, 2025 and took certain files."[13]

30. Defendant later determined that the files contained names, Social Security numbers, and driver's license numbers.[14]

[11] *Id.*

[12] *Id.*

[13] *See* Exhibit A.

[14] *Id.*

31. On or around March 17, 2026, Defendant reported the Data Breach to the California Office of the Attorney General[15] and the Office of the Maine Attorney General.[16] The Office of the Maine Attorney General disclosed that 19,075 Maine residents were impacted by the Data Breach.[17]

32. On or around March 18, 2026, the Texas Office of the Attorney General disclosed that 173,676 Texas residents were impacted by the Data Breach.[18]

33. The Data Breach Notices do not provide details about the root cause of the Data Breach, the vulnerabilities exploited, the criminals responsible for the breach, and the remedial measures undertaken to ensure such a breach does not occur again. To date, Defendant has not explained or disclosed these facts to Plaintiff and Class Members.

34. Without these details, Plaintiff's and Class Members' ability to mitigate harms resulting from the Data Breach is severely diminished.

35. Defendant's Data Breach notice offers no substantive steps to help victims like Plaintiff and Class Members to protect themselves other than providing identity protection, which is woefully inadequate considering the lifelong increased risk of fraud and identity theft that Plaintiff and Class Members now face as a result of the Data Breach.

---

[15] https://oag.ca.gov/system/files/Kaplan%20-%20California%20Notification.pdf (last visited April 1, 2026).

[16] *Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GEN. (MAR. 17, 2026), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/74143000-0a5a-4df2-81c9-5f41ef75619e.html (last visited April 1, 2026).

[17] *Id.*

[18] *Data Security Breach Reports*, TEXAS OFFICE OF THE ATTORNEY GENERAL, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited April 1, 2026).

36. Defendant has offered affected individuals 12 months of identity protection services through Experian IdentityWorks.[19] This limitation is inadequate when the victims will likely face many years of identity theft.

37. Moreover, Defendant's identity protection offer and advice to Plaintiff and Class Members squarely place the burden on Plaintiff and Class Members, rather than on Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant expects Plaintiff and Class Members to protect themselves from its tortious acts resulting from the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in identity protection services upon discovery of the Data Breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they could affirmatively take to protect themselves.

III. The Data Breach was Preventable

38. At all relevant times, Defendant knew, or should have known, that the PII it was entrusted with was a prime target for malicious actors. Defendant knew this given the unique type and the significant volume of data on its networks, servers, and systems, comprising individuals' detailed and confidential personal information and, thus, the significant number of individuals for whom the exposure of the unencrypted data would harm.

39. As custodian of Plaintiff's and Class Members' PII, Defendant knew or should have known the importance of protecting their PII, and of the foreseeable consequences and harms to such persons if any data breach occurred. Defendant's security obligations were also especially important due to the substantial increase of cyberattacks and data breaches in recent years, particularly those targeting businesses and other organizations like Defendant, which store and maintain large volumes of PII.

[19] *See* Exhibit A.

40. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[20] The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

41. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

42. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over the PII in its possession. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

IV. Defendant Failed to Comply with FTC Guidelines

43. At all times relevant to this Complaint, Defendant knew or should have known the significance and necessity of safeguarding the PII in its possession, and the foreseeable consequences of a data breach. Defendant knew or should have known that because it collected and maintained the PII for a significant number of individuals, a significant number of individuals would be harmed by a breach of their systems. Defendant further knew that the data it was entrusted with was highly valuable and contained private and sensitive information.

[20] 2021 Data Breach Annual Report, ITRC, https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last accessed April 3, 2025).

44. Because PII is so sensitive and cyberattacks have become a rising threat, the FTC has issued numerous guides for businesses holding sensitive PII and emphasized the importance of adequate data security practices. The FTC also stresses that appropriately safeguarding PII held by businesses should be factored into all business-related decision making.

45. An FTC Publication titled "Protecting Personal Information: A Guide for Business" lays out fundamental data security principles and standard practices that businesses should implement to protect PII.[21] The guidelines highlight that businesses should (a) protect the personal customer information they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems.

46. The FTC also recommends businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity, monitor for large amounts of data being transmitted from their systems, and have a response plan prepared in the event of a breach.

47. The FTC also recommends that businesses limit access to sensitive PII, require complex passwords to be used on the 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.

48. Businesses that do not comply with the basic protection of sensitive PII are facing enforcement actions brought by the FTC. Failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data is an unfair act or practice prohibited pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

[21] *See Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited June 30, 2025).

49. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

50. Defendant knew or should have known of its obligation to implement appropriate measures to protect Plaintiff's and Class Members' PII but failed to comply with the FTC's basic guidelines.

51. Defendant's failure to employ reasonable measures to adequately safeguard against unauthorized access to PII constitutes an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, as well as by state statutory analogs.

52. Once Defendant became aware of the breach, it could have acted far faster and more aggressively in responding to the breach and in assisting victims in redressing harms, including taking *any* steps whatsoever to attempt to mitigate the harm caused by the breach.

53. Identity thieves use such PII to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use this PII to open new financial accounts, open new utility accounts, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities." Additionally, identity thieves often wait significant amounts of time—months or even years—to use the PII obtained in data breaches because victims often become less vigilant in monitoring their accounts as time passes, therefore making the PII easier to use without detection. These identity thieves will also re-use stolen PII, resulting in victims of one data breach suffering the effects of several cybercrimes from one instance of unauthorized access to their PII.

V. Defendant Failed to Comply with Industry Standards

54. Security standards for businesses storing PII commonly include, but are not limited to:

a) Maintaining a secure firewall

b) Monitoring for suspicious or unusual traffic on the website

c) Looking for trends in user activity including for unknown or suspicious users

d) Looking at server requests for PII

e) Looking for server requests from VPNs and Tor exit nodes

f) Requiring Multi-factor authentication before permitting new IP addresses to access user accounts and PII

g) Structuring a system including design and control to limit user access as necessary, including a user's access to the account data and PII of other users.

55. Other best practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

56. Defendant failed to meet minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM- 06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIC CSC), which are all established standards in reasonable cybersecurity readiness.

57. These frameworks are existing and applicable industry standards which Defendant failed to comply with.

VI. Plaintiff's and Class Members' Experiences

58. Plaintiff received her Data Breach notice[22] dated March 17, 2026, informing her that her sensitive information was part of Defendant's Data Breach.

59. Plaintiff is unsure of her connection with Kaplan North America, and her Data Breach notice does not specify how Kaplan obtained her data.

60. Plaintiff's Wells Fargo bank account was hacked two to three months ago.

61. Defendant is in possession of Plaintiff's most sensitive personal information, and she cannot be sure how much of it was exfiltrated.

62. Plaintiff suffered an actual injury in the form of damages and diminution in the value of her PII—a form of tangible property that Plaintiff entrusted to Defendant, which was compromised in and because of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

63. Plaintiff has suffered imminent and impending injury arising from the heightened risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

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

VII. Defendant Breached Its Obligations to Plaintiff and the Class

[22] *See* Exhibit A.

65. Defendant fails to offer any compensation to victims of the Data Breach, who commonly face multiple years of ongoing identity theft, and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII, out-of-pocket costs, and the time taken by Plaintiff and Class Members to mitigate their injuries.

66. Plaintiff and Class Members have been damaged by the compromise and exfiltration by cybercriminals of their PII as a result of the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of the Data Breach.

67. Plaintiff and Class Members were damaged since their PII is being sold or potentially for sale by cybercriminals in the years to come.

68. As a direct and proximate consequence of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, actual, and substantial risk of harm from fraud and identity theft, especially considering the actual fraudulent misuse of the PII that has already taken place.

69. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

70. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, and similar identity theft. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

71. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

72. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cybercriminals in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

73. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

74. Many Class Members suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a) Finding fraudulent charges;

b) Cancelling and reissuing credit and debit cards;

c) Purchasing credit monitoring and identity theft prevention;

d) Monitoring their medical records for fraudulent charges and data;

e) Addressing their inability to withdraw funds linked to compromised accounts;

f) Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g) Placing "freezes" and "alerts" with credit reporting agencies;

h) Spending time on the phone with or at a financial institution to dispute fraudulent charges;

i) Contacting financial institutions and closing or modifying financial accounts;

j) Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

k) Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l) Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

75. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

CLASS ACTION ALLEGATIONS

76. Plaintiff brings this class action on behalf of herself and all other similarly situated individuals under Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3), on behalf of the following Class:

> All individuals within the United States whose PII was identified as compromised in the Data Breach.

77. Excluded from the Class are governmental entities, Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded from the Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

78. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements therein.

79. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. Upon information and belief, the Class contains hundreds of thousands of individuals and is sufficiently numerous to warrant certification.

80. **Commonality.** Common legal and factual questions exist that predominate over any questions affecting only individual Class Members. These common questions, which do not vary among Class Members and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to:

a) Whether Defendant failed to take adequate and reasonable measures to ensure its website and data systems were protected;

b) Whether Defendant failed to take available steps to prevent and stop the Data Breach from happening or mitigating the risk of a long-term breach;

c) Whether Defendant unreasonably delayed in notifying Plaintiff and Class Members of the harm they suffered once the suspicious activity was detected;

d) Whether Defendant owed a legal duty to Plaintiff and Class Members to protect their PII;

e) Whether Defendant breached any duty to protect the personal information of Plaintiff and Class Members by failing to exercise due care in protecting their PII;

f) Whether Defendant took sufficient steps to secure Class Members' PII;

g) Whether Defendant was unjustly enriched;

h) Whether Plaintiff and Class Members are entitled to actual, statutory, or other forms of damages and other monetary relief; and,

i) Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief or restitution.

81. **Typicality.** Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

82. **Adequacy of Representation.** Plaintiff is an adequate class representative because she is a Class Member, and her interests do not conflict with the Class's interests. Plaintiff retained counsel who are competent and experienced in class action and data breach litigation. Plaintiff and her counsel intend to prosecute this action vigorously for the Class's benefit and will fairly and adequately protect her and the Class's interests.

83. **Predominance and Superiority.** The Class can be properly maintained because the above common questions of law and fact predominate over any questions affecting individual Class Members. A class action is also superior to other available methods for the fair and efficient adjudication of this litigation because individual litigation of each Class Member's claim is impracticable. Even if each Class Member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

84. **Declaratory and Injunctive Relief.** The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect

to individual Class Members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their interests. Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

CLAIMS FOR RELIEF

Count 1
Negligence
On behalf of Plaintiff and the Class

85. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

86. Plaintiff and Class Members entrusted their PII to Defendant with the understanding that it would safeguard their PII.

87. Defendant had full knowledge of the sensitivity of the PII that it stored and the types of harm that Plaintiff and Class Members could and would suffer if that PII were wrongfully disclosed.

88. Defendant violated its duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing Defendant's information security controls sufficiently rigorously to ensure that PII in its possession was adequately secured by, for example, encrypting sensitive personal information, installing effective intrusion detection systems and monitoring mechanisms, using access controls to limit access to sensitive data, regularly testing for security weaknesses and failures, failing to notify victims of the specific breached data in a timely manner, and failing to remedy the continuing harm by unreasonably delaying notifying specific victims who were harmed.

89. Defendant's duty of care arose from, among other things,

a) The special relationship between Defendant, Plaintiff, and Class Members resulting from Plaintiff and Class Members entrusting Defendant with confidential PII;

b) Defendant's exclusive ability (and Class Members' inability) to ensure that its systems, website, and vendor services were sufficient to protect against the foreseeable risk that a data breach could occur;

c) Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures; and

d) Defendant's common law duties to adopt reasonable data security measures to protect PII under its possession and to act under the same or similar circumstances as a reasonable and prudent person would act.

90. Plaintiff and Class Members were the foreseeable victims of Defendant's inadequate data security. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches. Defendant knew that a breach of its systems could and would cause harm to Plaintiff and Class Members.

91. Defendant's conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's conduct included its failure to adequately mitigate harm through negligently failing to inform victims of the breach of the specific information breached.

92. Defendant knew or should have known of the inherent risks in collecting and storing massive amounts of PII and the importance of limiting disclosure of that PII.

93. Defendant, through its actions and inactions, breached its duty owed to Plaintiff and Class Members by failing to exercise reasonable care in safeguarding their PII while it was in

its possession and control. Defendant breached its duty by, among other things, its failure to adopt reasonable data security practices and its failure to adopt reasonable security and notification practices, failure to monitor the security of its networks and systems, and allowing unauthorized access to Plaintiff's and Class Members' PII.

94. Defendant inadequately safeguarded PII in breach of standard industry rules, regulations, and best practices at the time of the Data Breach.

95. But for Defendant's breach of its duty to adequately protect Class Members' PII, Class Members' PII would not have been stolen.

96. There is a temporal and close causal connection between Defendant's failure to implement adequate data security measures and notification practices, the Data Breach/unauthorized disclosure, and the harms suffered by Plaintiff and Class Members.

97. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their PII had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

98. As a direct and traceable result of Defendant's negligence, Plaintiff and Class Members suffered and will continue to suffer damages, including monetary damages, increased risk of future harm, loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach, overpayment for the services and products that were received without adequate data security; and embarrassment, humiliation, and emotional distress.

99. Plaintiff and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate identity protection services. Plaintiff and Class Members are also entitled to the injunctive relief sought herein.

100. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 2
Negligence *Per Se*
On behalf of Plaintiff and the Class

101. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

102. Section 5 of the FTC Act, 15 U.S.C. § 45 prohibits, "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiff's and Class Members' PII.

103. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and by failing to comply with industry standards.

104. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems. Plaintiff was required to provide PII to Defendant. Plaintiff and Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their PII.

105. Class Members are within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

106. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

107. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

108. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it failed to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

109. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

Count 3
Breach of Implied Contract
On behalf of Plaintiff and the Class

110. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

111. Plaintiff and other Class Members entered into an implied contract with Defendant when they entrusted Defendant with their PII.

112. Plaintiff and Class Members entrusted their PII to Defendant. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect PII, and to timely and accurately notify Plaintiff and the Class if their data has been breached and compromised or stolen.

113. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

114. Implicit in the agreement between Plaintiff, Class Members, and Defendant to provide PII, was Defendant's obligation to: (1) use such PII for business purposes only, (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' PII, (3) prevent unauthorized disclosures of the PII, and (4) retain PII only under conditions that kept such information secure and confidential.

115. As part of these transactions, Defendant agreed to safeguard and protect the PII of Plaintiff and Class Members and to timely and accurately notify them if their PII was breached or compromised.

116. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with the legal requirements, industry standards, and Defendant's own representations.

117. Implicit in the agreement between Defendant, Plaintiff, and Class Members, was the obligation that all parties would maintain information confidentially and securely.

118. These exchanges constituted an agreement and meeting of the minds between the parties.

119. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have provided and entrusted their PII to Defendant in the absence of the implied contract or implied terms between them and Defendant. The safeguarding of the PII of Plaintiff and Class Members was critical to realize the intent of the parties.

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

121. Defendant breached its implied contracts with Plaintiff and Class Members to protect their PII when it (1) failed to take reasonable steps to use safe and secure systems to protect

that information; (2) failed to comply with industry standards; (3) failed to comply with the legal obligations necessarily incorporated into these agreements; and (4) failed to notify Plaintiff and Class Members of the specific data breached in a reasonably timely manner.

122. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

123. As a direct and proximate result of the breach/unauthorized disclosure, Plaintiff and Class Members are entitled to relief as set forth herein.

124. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 4
Unjust Enrichment
On behalf of Plaintiff and the Class

125. Plaintiff, individually and on behalf of the Class, incorporates by reference each of the factual allegations contained in the preceding paragraphs as if fully set forth herein.

126. This count is brought in the alternative to Plaintiff's breach of contract claim.

127. Plaintiff and Class Members conferred a benefit on Defendant by providing their PII to Defendant and obtaining educational services from Defendant.

128. Upon information and belief, the monies paid to Defendant in the ordinary course of business included a premium for Defendant's cybersecurity obligations and were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiff's and Class Members' PII.

129. Defendant, however, failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

130. Defendant would not be able to carry out an essential function of its regular business without the money obtained in the ordinary course of business and PII provided by Plaintiff and Class Members. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

131. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

132. Defendant knew that Plaintiff and Class Members conferred a benefit upon it, which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes, while failing to use the payments it received for

adequate data security measures that would have secured Plaintiff's and Class Members' PII and prevented the Data Breach.

133. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII, they would not have provided their PII to Defendant.

134. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and cheaper contractors and diverting those funds to its own profits. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their PII.

135. Under the principles of equity and good conscience, Defendant should not be permitted to retain the benefits that Plaintiff and Class Members conferred upon it.

136. Plaintiff and Class Members have no adequate remedy at law.

137. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injuries described herein.

138. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid to Defendant.

139. Plaintiff also seeks such other relief as the Court may deem just and proper.

Count 5
Injunctive/Declaratory Relief
On behalf of Plaintiff and the Class

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

141. Defendant owes a duty of care to Plaintiff and Class Members, which required Defendant to adequately monitor and safeguard Plaintiff's and Class Members' PII.

142. Defendant and its officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the PII belonging to Plaintiff and Class Members.

143. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and the Class continue to suffer injury as a result of the compromise of their PII and the risk remains that further compromises of their PII will occur in the future.

144. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a) Defendant owes a legal duty to adequately secure the PII of Plaintiff and the Class within its care, custody, and control under the common law, and Section 5 of FTC Act;

b) Defendant breached its duty to Plaintiff and the Class by allowing the Data Breach to occur;

c) Defendant's existing data monitoring measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the PII of Plaintiff and the Class within Defendant's custody, care, and control; and

d) Defendant's ongoing breaches of said duties continue to cause harm to Plaintiff and the Class.

145. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect the PII of Plaintiff and the Class within its custody, care, and control, including the following:

a) Order Defendant to provide lifetime credit monitoring and identity theft insurance and protection services to Plaintiff and Class Members; and

b) Order that, to comply with Defendant's obligations and duties of care, Defendant must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems, networks, and servers on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Encrypting and anonymizing the existing PII within its servers, networks, and systems to the extent practicable, and purging all such information which is no

longer reasonably necessary for Defendant to provide services to its employees or customers;

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training its security personnel regarding any new or modified procedures;

v. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems, networks, and servers;

vi. Conducting regular database scanning and security checks; and

vii. Routinely and continually conducting internal training and education to inform Defendant's internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

146. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If another data breach or cybersecurity incident occurs, Plaintiff and the Class will not have an adequate remedy at law because monetary relief alone will not compensate Plaintiff and the Class for the serious risks of future harm.

147. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff and the Class will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable

prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

148. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach or cybersecurity incident, thus preventing future injury to Plaintiff and the Class and other persons whose PII would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action and appoint Plaintiff and her counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the PII of Plaintiff and the Class by implementing improved security controls;

C. That the Court award compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

D. That the Court award statutory or punitive damages as allowed by law in an amount to be determined at trial;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of Defendant's unlawful acts, omissions, and practices;

F. That the Court award to Plaintiff and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate; and

H. All such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all claims so triable.

Dated: April 1, 2026

Respectfully submitted,

/s/ Francesca Burne
Francesca Burne (FL Bar No. 1021991)
AYLSTOCK, WITKIN, KREIS & OVERHOLTZ, PLC
17 E. Main Street, Suite 200
Pensacola, FL 32502
Tel: (850) 266-2989
Fburne@awkolaw.com

/s/ Sonum Dixit
Sonum Dixit* (CA Bar No. 353395)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St, Ste 200
San Francisco, CA 94123
Tel: 415-788-4220
Fax: 415-788-0161
sdixit@sjk.law

Counsel for Plaintiff and the Proposed Class

*pro hac vice forthcoming