William B. Federman (*pending pro hac vice)*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com

[Additional counsel appears on the signature page]

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

TARA McINTOSH, individually and on behalf of all others similarly situated, Plaintiff, vs. HOPSKIPDRIVE, INC., Defendant.	Case No. 2:24-cv-1676 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Tara McIntosh, by and through her counsel, brings this Class Action Complaint against Defendant HopSkipDrive, Inc., individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. Plaintiff Tara McIntosh ("Plaintiff") brings this class action against Defendant HopSkipDrive, Inc. ("Defendant") for its failure to properly secure and safeguard sensitive information that Plaintiff and Class Members, as customers and employees of Defendant, entrusted to it, including, without limitation: their names, addresses, email addresses, dates of

birth, driver's license numbers, Social Security numbers, and medical information (collectively, "Personal Information" or "PII and PHI").

2. Defendant is a ridesharing company that provides transportation service to schools and families.[1]

3. Plaintiff and Class Members are current and former customers and employees of Defendant consisting of approximately 155,394 individuals.

4. As a condition of receiving its services, Defendant requires that its customers and employees, including Plaintiff and Class Members, entrust it with highly sensitive Personal Information, including but not limited to their names, addresses, email addresses, dates of birth, driver's license numbers, Social Security numbers, and medical information.

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

6. Defendant derives a substantial economic benefit from collecting Plaintiff's and Class Members' Personal Information. Without it, Defendant could not perform its services.

7. Defendant had a duty to adopt reasonable measures to protect the Personal Information of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its third-party applications and affiliates for their own cybersecurity. Defendant has a legal duty to keep consumer's Personal Information safe and confidential.

8. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Personal Information, Defendant assumed legal and equitable duties to ensure the protection of that Personal Information, and it knew or should have known that it was thus responsible for protecting Plaintiff's and Class Members' Personal Information from disclosure.

[1] *See* https://www.hopskipdrive.com/about (last visited February 7, 2024).

9. On or about November 14, 2023, Defendant began sending Plaintiff and Class Members a Notice of Data Breach (the "Notice Letter") informing them that their Personal Information had been exposed when an unknown and unauthorized individual accessed certain third-party applications utilized by Defendant between May 31, 2023, and June 10, 2023 and stole Plaintiff's and Class Members' Personal Information (the "Data Breach").

10. Noticeably absent from the Notice Letter are details of the root cause of the Data Breach, the vulnerabilities that were exploited, and the remedial measures that Defendant undertook to ensure such a breach does not happen again. To date, these critical facts have not been explained or clarified to Plaintiff or Class Members, who have a vested interest in ensuring that their Personal Information remains protected.

11. In fact, the attacker accessed and acquired files that Defendant shared with its third-party applications containing unencrypted Personal Information of Plaintiff and Class Members, including their Social Security numbers and medical information.

12. To make matters even worse, Defendant waited almost four full months after it became aware of the Data Breach, and more than five months after the actual Data Breach, to begin to notify the individuals affected by the Data Breach including Plaintiff and Class Members.

13. Plaintiff brings this action on behalf of all persons whose Personal Information was compromised as a result of Defendant's failure to: (i) adequately protect the Personal Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware and software containing protected Personal Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to, among other things, negligence and violates federal and state statutes.

14. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of Personal Information; (ii) out-of-

pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (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 Personal Information; and (v) the continued and certainly increased risk to their Personal Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information.

15. Defendant 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 Personal Information 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 a result, the Personal Information of Plaintiff and Class Members was compromised through disclosure to an unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

II. PARTIES

16. Plaintiff Tara McIntosh is, and at all times relevant, has been a resident and citizen of Spokane, Washington. Plaintiff McIntosh has no intention of moving to a different state in the immediate future.

17. Defendant HopSkipDrive, Inc. is a California-based corporation with its principal place of business at 360 East 2nd Street, Ste 325, Los Angeles, California 90012.

III. JURISDICTION AND VENUE

18. This Court has diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class

members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant, including the Plaintiff.

19. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and it regularly transacts business in this District.

20. Venue as to Defendant is proper in this judicial district under 28 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District and many of Defendant's acts complained of herein occurred within this District.

IV. FACTUAL BACKGROUND

A. The Data Breach

21. On November 14, 2023, more than three months discovering the Data Breach and more than five (5+) months after the Data Breach, Defendant sent Notices of Data Breach to its customers and employees that were affected by the Data Breach.[2] According to the Notice of Data Breach, "[o]n or about July 25, 2023, HopSkipDrive received an email communication from an unknown individual claiming to have accessed certain third-party applications utilized by HopSkipDrive."[3] Defendant collaborated with a third-party investigation company that "determined the [Data Breach] occurred between May 31, 2023 and June 10, 2023."[4]

22. As a result of the Data Breach, Plaintiff's and Class Members' Personal Information has been exposed to cybercriminals. This Personal Information includes, but is not limited to, Plaintiff's and Class Members' names, addresses, email addresses, dates of birth, driver's license numbers, Social Security numbers, and medical information.[5]

23. Defendant had obligations to Plaintiff and to Class Members to safeguard their Personal Information and to protect that Personal Information from unauthorized access and disclosure, including by ensuring that its third-party applications had information security

[2] *See* Notice of Data Breach addressed to Plaintiff dated November 14, 2023 attached hereto as **Exhibit 1**.
[3] *Id.*
[4] *Id.*
[5] *Id.*

practices and protocols in place that would protect that Personal Information. Indeed, Plaintiff and Class Members provided their Personal Information to Defendant with the reasonable expectation, and mutual understanding, that Defendant, and anyone Defendant contracted with, would comply with its obligations to keep such information confidential and secure from unauthorized access. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches of major companies before the Data Breach.

24. Defendant also had obligations to promptly notify Plaintiff and Class Members of the Data Breach in a timely manner, which it has clearly failed to do waiting more than three months after being notified of the Data Breach and more than five months after the Data Breach to notify affected individuals of their Personal Information being exposed.

25. Defendant also promises it will safeguard users' privacy in its *Privacy Policy*.[6] Specifically, Defendant's *Privacy Policy* provides in relevant part:

> **Data Security.** HopSkipDrive has implemented administrative, technical, and physical security controls designed to safeguard personal information.[7]

26. Indeed, Defendant has failed to uphold its duty and promise to safeguard Plaintiff and Class Members' Personal Information.

27. In response to the Data Breach, Defendant is urging affected consumers to "remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information."[8]

B. Plaintiff Expected HopSkipDrive and its Third-Party Applications to Keep Her Information Secure.

Plaintiff Tara McIntosh's Experience

[6] *See* HopSkipDrive, Inc.'s *Privacy Notice*, *available* at https://www.hopskipdrive.com/privacy (Last visited December 14, 2023).
[7] *Id*.
[8] *See Supra*, at Note No. 2.

28. Plaintiff McIntosh provided her Personal Information, at Defendant's request, when she was hired by Defendant on or around May of 2023.

29. Plaintiff McIntosh is very careful about sharing her sensitive Personal Information. Plaintiff McIntosh has never knowingly transmitted unencrypted sensitive Personal Information over the internet or any other unsecured source.

30. Plaintiff McIntosh first learned of the Data Breach after she received a Notice of Data Breach letter from Defendant on or around November 14, 2023, notifying her that her Personal Information had been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendant. Defendant revealed that the Data Breach occurred between May 31, 2023, and June 10, 2023, and Defendant only discovered it roughly one to two months afterward.[9]

31. As a result of the Data Breach, Plaintiff McIntosh made reasonable efforts to mitigate the impact of the Data Breach after receiving the Notice of Data Breach letter, including but not limited to researching the Data Breach, reviewing credit reports, and financial account statements for any indications of actual or attempted identity theft or fraud.

32. Plaintiff McIntosh has spent multiple hours and will continue to spend valuable time for the remainder of her life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation. Since Plaintiff McIntosh became aware of the Data Breach, she has spent hours trying to fix issues stemming from the Data Breach.

33. Plaintiff McIntosh suffered actual injury from having her Personal Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Personal Information, a form of property that Defendant maintained belonging to Plaintiff McIntosh; (b) violation of her privacy rights; (c) the theft of her Personal Information; and (d) present, imminent and impending injury arising from the

[9] *Id.*

increased risk of identity theft and fraud. In fact, because her Social Security number was impacted, Plaintiff McIntosh faces this risk for the rest of her life.

34. As a result of the Data Breach, Plaintiff McIntosh anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. In addition, Plaintiff McIntosh will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

C. FTC Security Guidelines Concerning PII

35. The Federal Trade Commission ("FTC") has established security guidelines and recommendations to help entities protect PII and reduce the likelihood of data breaches.

36. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

37. In 2016, the FTC provided updated security guidelines in a publication titled Protecting Personal Information: A Guide for Business. Under these guidelines, companies should protect consumer information they keep; limit the sensitive consumer information they keep; encrypt sensitive information sent to third parties or stored on computer networks; identify and understand network vulnerabilities; regularly run up-to-date anti-malware programs; and pay particular attention to the security of web applications—the software used to inform visitors to a company's website and to retrieve information from the visitors.

38. The FTC recommends that businesses do not maintain payment card information beyond the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the

industry; and verify that third parties with access to sensitive information use reasonable security measures.

39. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

40. The FTC has brought several actions to enforce Section 5 of the FTC Act. According to its website:

> When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights or misled them by failing to maintain security for sensitive consumer information or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.[10]

41. Defendant was aware or should have been aware of its obligations to protect its customers' and employees' Personal Information, including both PII and PHI, and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers and employees from unauthorized access. Among other violations, Defendant violated its obligations under Section 5 of the FTC Act.

/ / /

/ / /

D. HopSkipDrive, Inc. Was on Notice of Data Threats and the Inadequacy of Its Third-party applications' Data Security.

[10] *See* Fed. Trade Comm'n, *Privacy and Security Enforcement*, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited December 14, 2023).

42. Defendant was on notice that companies maintaining large amounts of Personal Information during their regular course of business are prime targets for criminals looking to gain unauthorized access to sensitive and valuable information, such as the type of data at issue in this case.

43. At all relevant times, Defendant knew, or should have known, that the Personal Information that it collected was a target for malicious actors. Despite such knowledge, and well-publicized cyberattacks on similar companies, Defendant failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Personal Information from cyber-attacks that Defendant should have anticipated and guarded against.

44. In light of recent high profile data breaches, including Microsoft (250 million records, December 2019), T-Mobile (110 million records, August 2021), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

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

E. The Data Breach Harmed Plaintiff and Class Members

46. Plaintiff and Class Members have suffered and will continue to suffer harm because of the Data Breach.

47. Plaintiff and Class Members face a present and imminent and substantial risk of injury of identity theft and related cyber crimes due to the Data Breach for their respective lifetimes. Once data is stolen, malicious actors will either exploit the data for profit themselves or sell the data on the dark web to someone who intends to exploit the data for profit. Hackers

would not incur the time and effort to steal PII and PHI—thereby risking prosecution by listing it for sale on the dark web—if the PII and PHI was not valuable to malicious actors.

48. The dark web helps ensure users' privacy by effectively hiding server or IP details from the public. Users need special software to access the dark web. Most websites on the dark web are not directly accessible via traditional searches on common search engines and are therefore accessible only by users who know the addresses for those websites.

49. Malicious actors use PII and PHI to gain access to Class Members' digital life, including bank accounts, social media, and credit card details. During that process, hackers can harvest other sensitive data from the victim's accounts, including personal information of family, friends, and colleagues.

50. Consumers are injured every time their data is stolen and placed on the dark web, even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of multiple discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

51. Without giving any details, Defendant has also vaguely stated that it "received an email communication from an unknown individual claiming to have accessed certain third-party applications utilized by HopSkipDrive" and "promptly launched an investigation […]"[11] Defendant also stated that they engaged with "experts to assist in assessing the scope of the incident and took steps to mitigate […]" again, without giving any details of who these advisors were, how they assisted, or any details about the Data Breach and the steps they took to ensure Plaintiff's and Class Members' Personal Information cannot be accessed against.[12] Indeed, Plaintiff and Class Members are thus left to guess whether Defendant has, in fact, addressed the

[11] *See Supra*, at Note No. 2.
[12] *Id.*

root causes of the Data Breach to ensure that Plaintiff and Class Members' Personal Information cannot be accessed again.

52. Defendant's intentionally misleading public statements ignore the serious harm its security flaws caused to Plaintiff and Class Members. Even worse, those statements could convince Class Members that they do not need to take steps to protect themselves.

53. The data security community agrees that the Personal Information compromised in the Data Breach greatly increases Class Members' risk of identity theft and fraud.

54. As Justin Fier, senior vice president for AI security company Darktrace, observed following a recent data breach at T-Mobile, "[t]here are dozens of ways that the information that was stolen could be weaponized." He added that such a massive treasure trove of consumer profiles could be of use to everyone from nation-state hackers to criminal syndicates.[13]

55. Criminals can use the Personal Information that Defendant lost to target Class Members for imposter scams, a type of fraud initiated by a person who pretends to be someone the victim can trust in order to steal sensitive data or money.[14]

56. The Personal Information accessed in the Data Breach therefore has significant value to the hackers that have already sold or attempted to sell that information and may do so again.

57. Malicious actors can also use Class Members' Personal Information to open new financial accounts, open new utility accounts, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."

---

[13] *See* Bree Fowler, *T-Mobile Gets Hacked Again: Is the Un-Carrier Un-Safe?*, https://www.cnet.com/tech/services-and-software/t-mobile-gets-hacked-again-is-the-un-carrier-un-safe/ (last visited December 14, 2023).

[14] *See* Fed. Trade Comms'n, *How to Avoid Imposter Scams*, https://consumer.ftc.gov/features/imposter-scams (last visited December 14, 2023).

58. As established above, the Personal Information accessed in the Data Breach is also very valuable to Defendant. Defendant collects, retains, and uses this information to increase its profits. Defendant's customers and employees both value the privacy of this information and expect Defendant to allocate enough resources to ensure it is adequately protected. The decision of customers to engage with the Defendant, and of employees to work for them, is contingent on the assumption that the Defendant employs reasonable security measures for Personal Information. Had they been aware of any shortcomings in these measures, customers would have reconsidered their transactions, or the prices paid for the Defendant's goods and services, while employees would have reevaluated their employment choices. Both customers and employees reasonably expect that their payments or wages incorporate the costs of implementing such security measures, as part of the overall commitment to protecting their Personal Information and upholding their privacy.

59. Indeed, "[f]irms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[15] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[16] It is so valuable to identity thieves that once Personal Information has been disclosed, criminals often trade it on the "cyber black-market" or the "dark web" for many years.

60. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, PHI, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data

[15] *See* OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, No. 220, Apr. 2, 2013, https://doi.org/10.1787/5k486qtxldmq-en (last visited December 14, 2023).

[16] *See* IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited December 14, 2023).

Breach, can be readily aggregated, and it can become more valuable to thieves and more damaging to victims.

61. The Personal Information accessed in the Data Breach is also very valuable to Plaintiff and Class Members. Consumers often exchange personal information for goods and services. For example, consumers often exchange their personal information for access to wifi in places like airports and coffee shops. Likewise, consumers often trade their names and email addresses for special discounts (e.g., sign-up coupons exchanged for email addresses). Consumers use their unique and valuable Personal Information to access the financial sector, including when obtaining a mortgage, credit card, or business loan. As a result of the Data Breach, Plaintiff and Class Members' Personal Information has been compromised and lost significant value.

62. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[17]

63. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Personal Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

64. Due to the immutable nature of the personal information impacted here, Plaintiff and Class Members will face a risk of injury due to the Data Breach for their respective lifetimes. Malicious actors often wait months or years to use the personal information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen personal

[17] *See* Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RES. 254 (June 2011) https://www.jstor.org/stable/23015560 (last visited December 14, 2023).

information, meaning individuals can be the victim of several cyber crimes stemming from a single data breach. Finally, there is often significant lag time between when a person suffers harm due to theft of their Personal Information and when they discover the harm. For example, victims rarely know that certain accounts have been opened in their name until contacted by collections agencies. Plaintiff and Class Members will therefore need to continuously monitor their accounts for years to ensure their Personal Information obtained in the Data Breach is not used to harm them.

65. Even when reimbursed for money stolen due to a data breach, consumers are not made whole because the reimbursement fails to compensate for the significant time and money required to repair the impact of the fraud.

66. Victims of identity theft also experience harm beyond economic effects. According to a 2018 study by the Identity Theft Resource Center, 32% of identity theft victims experienced negative effects at work (either with their boss or coworkers) and 8% experienced negative effects at school (either with school officials or other students).

67. The U.S. Government Accountability Office likewise determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[18]

68. Plaintiff and Class Members have failed to receive the value of the Defendant's services for which they paid.

F. Defendant Failed to Take Reasonable Steps to Protect its Customers' and Employees' Personal Information

69. Defendant requires its customers and employees to provide a significant amount of highly personal and confidential Personal Information to purchase or utilize its services.

[18] *See* GAO, *Personal Information Data Breaches are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent is Unknown*, https://www.gao.gov/assets/gao-07-737.pdf (last visited December 14, 2023).

Defendant collects, stores, and uses this data to maximize profits while failing to encrypt or protect it properly.

70. Defendant has legal duties to protect its customers' and employees' Personal Information by implementing reasonable security features. This duty is further defined by federal and state guidelines and laws, including the FTC Act, as well as industry norms.

71. Defendant breached its duties by failing to implement reasonable safeguards to ensure Plaintiff's and Class Members' Personal Information was adequately protected. As a direct and proximate result of this breach of duty, the Data Breach occurred, and Plaintiff and Class Members were harmed.

72. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Personal Information of Plaintiff and Class Members and ensuring that its third-party applications did so as well.

73. Defendant's negligence in safeguarding the Personal Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

74. Experts have identified several best practices that businesses like Defendant should implement at a minimum, including, but not limited to educating all employees; requiring strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

75. Other best cybersecurity 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; and training staff regarding critical points.

76. When using a third-party application, moreover, best cybersecurity practices include not storing data or information longer than necessary to accomplish the intended business purpose. By storing Plaintiff's and Class Members' Personal Information longer than was necessary to accomplish the intended business purpose, Defendant's third-party application—for whom Defendant was responsible—left Plaintiff's and Class Members' Personal Information vulnerable to access and theft, which is what ultimately happened.

77. The Data Breach was a reasonably foreseeable consequence of Defendant's failure to ensure that its third-party application used adequate security systems. Defendant certainly has the resources to ensure that its third-party application implement reasonable security systems to prevent or limit damage from data breaches. Even so, Defendant failed to properly invest in that data security. Had Defendant ensured that its third-party application implemented reasonable data security systems and procedures (i.e., followed guidelines from industry experts and state and federal governments), then it likely could have prevented hackers from accessing its customers' and employees' Personal Information.

78. Defendant's failure to ensure that its third-party application implemented reasonable security systems has caused Plaintiff and Class Members to suffer and continue to suffer harm that adversely impact Plaintiff and Class Members economically, emotionally, and/or socially. As discussed above, Plaintiff and Class Members now face a substantial, imminent, and ongoing threat of identity theft, scams, and resulting harm. These individuals now must spend significant time and money to continuously monitor their accounts and credit scores and diligently sift out phishing communications to limit potential adverse effects of the Data Breach, regardless of whether any Class Member ultimately falls victim to identity theft.

79. In sum, Plaintiff and Class Members were injured as follows: (i) theft of their Personal Information and the resulting loss of privacy rights in that information; (ii) improper disclosure of their Personal Information; (iii) diminution in value of their Personal Information; (iv) the certain, ongoing, and imminent threat of fraud and identity theft, including the economic

and non-economic impacts that flow therefrom; (v) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; and/or (vi) nominal damages.

80. Even though Defendant has decided to offer free credit monitoring for twelve (12) months to affected individuals, this is insufficient to protect Plaintiff and Class Members. As discussed above, the threat of identity theft and fraud from the Data Breach will extend for many years and cost Plaintiff and Class Members significant time and effort.

81. Plaintiff and Class Members therefore have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages) that protects them from these long-term threats. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

V. CLASS ACTION ALLEGATIONS

82. Plaintiffs bring this class action on behalf of a Nationwide Class according to Federal Rules of Civil Procedure, Rules 23(b)(2), 23(b)(3), and 23(b)(4). The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> **All citizens of the United States who received a Notice of Data Breach letter from HopSkipDrive, Inc., on or about November 14, 2023 (the "Class").**

83. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; all individuals who are California citizens and/or residents; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

84. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

85. Numerosity: Class Members are so numerous that joinder of all members is impracticable, if not completely impossible. According to the Office of the Maine Attorney General the total number of persons affected in the Data Breach is 155,394.

86. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any questions affecting solely individual Class Members. Among the questions of law and fact common to Class Members that predominate over questions which may affect individual Class members, including the following:

a. Whether Defendant owed a duty to Plaintiff and Class Members to exercise due care in collecting, storing, safeguarding and/or obtaining their Personal Information;

b. Whether Defendant breached that duty;

c. Whether Plaintiff's and Class Members' Personal Information was accessed and/or viewed by one or more unauthorized persons in the Data Breach alleged above;

d. When and how Defendant should have learned and actually learned of the Data Breach;

e. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Personal Information had been compromised;

f. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Personal Information had been compromised;

g. Whether Defendant's response to the Data Breach was adequate;

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

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

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

k. Whether an implied contract existed between Defendant and Plaintiff and Class Members;

l. Whether Defendant breached its implied contract with Plaintiff and Class Members;

m. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

n. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

o. Whether Plaintiff and Class Members are entitled to equitable relief;

p. 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.

q. Whether Defendant was unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

87. Typicality: Plaintiff's claims are typical of those of the other Class Members because Plaintiff, like every other member, was exposed to virtually identical conduct and now suffers from the same violations of the law as other Class Members.

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

89. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

90. Superiority and Manageability: 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 a large corporation, like Defendant. Further, even for

those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

91. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by Class Members 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.

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

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

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

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and Class Members)

95. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

96. Defendant requires its customers and employees, including Plaintiff and Class Members, to submit non-public Personal Information in the ordinary course of providing its services.

97. Defendant gathered, stored, and shared the Personal Information of Plaintiff and Class Members, who are the customers and employees of Defendant, as an integral part of its business activities. This was crucial to both providing services and soliciting customers, which affect commerce.

98. Plaintiff and Class Members entrusted Defendant with their Personal Information, directly or indirectly, with the understanding that Defendant would safeguard their information.

99. Defendant had full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiff and Class Members could and would suffer if the Personal Information were wrongfully disclosed.

100. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to exercise due diligence in selecting third-party application and to audit, monitor, and ensure the integrity of its third-party application' systems and practices and to give prompt notice to those affected in the case of a data breach.

101. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

102. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to

ensure that its and its third-party application's systems and networks, and the personnel responsible for them, adequately protected the Personal Information.

103. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Plaintiff and Class Members entrusted Defendant with their confidential Personal Information, a necessary part of being customers and employees of Defendant.

104. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Personal Information.

105. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or Class Members.

106. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' and employees' Personal Information when it was no longer required to retain pursuant to regulations.

107. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

108. Defendant had and continues to have a duty to adequately disclose that the Personal Information of Plaintiff and Class Members within its or its third-party application's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was and is necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Personal Information by third parties.

109. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's

and Class Members' Personal Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Personal Information;

b. Failing to adequately monitor the security of its and its third-party application's networks and systems;

c. Failing to audit, monitor, or ensure the integrity of its third-party application's data security practices;

d. Allowing unauthorized access to Plaintiff's and Class Members' Personal Information;

e. Failing to detect in a timely manner that Plaintiff's and Class Members' Personal Information had been compromised;

f. Failing to remove former customers' and employees' Personal Information it was no longer required to retain pursuant to regulations; and

g. Failing to timely and adequately notify Plaintiff and Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

110. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

111. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

112. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

113. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

114. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

115. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' Personal Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in Defendant's industry.

116. Defendant has full knowledge of the sensitivity of the Personal Information and the types of harm that Plaintiff and Class Members could and would suffer if the Personal Information were wrongfully disclosed.

117. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Personal Information of Plaintiff and Class Members, the critical importance of providing adequate security of that Personal Information, and the necessity for encrypting Personal Information stored on its and its third-party application's systems.

118. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' Personal Information would result in one or more types of injuries to Plaintiff and Class Members.

119. Plaintiff and Class Members had no ability to protect their Personal Information that was in, and possibly remains in, Defendant's and its third-party provider's possession.

120. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach. However, Plaintiff and Class Members had no ability to protect their Personal Information in Defendant's possession.

121. Defendant's duty extended to protecting Plaintiff and Class Members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

122. Defendant has admitted that the Personal Information of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

123. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the Personal Information of Plaintiff and Class Members would not have been compromised.

124. There is a close causal connection between Defendant's failure to implement security measures to protect the Personal Information of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The Personal Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Personal Information by adopting, implementing, and maintaining appropriate security measures.

125. Defendant's conduct, as alleged herein, allowed it to gain a competitive advantage over companies offering the same or similar services because, rather than properly implement data security protocols, or verify the integrity of its third-party application's systems, as required by statute and industry standards, Defendant diverted money intended to apply to data security towards its own profit. Defendant's conduct, and the unfair advantage realized

thereby, creates a race to the bottom by encouraging companies to divert funds intended for data security towards profits in order to remain competitive. The end effect is that both consumers and the marketplace in general are harmed through the widespread adoption of substandard data security practices and the concomitantly increased risk of cyberattacks and fraud and identity theft (which disrupt the lives of victims and impose a burden on the state to investigate and prevent criminal activity).

126. By collecting and taking custody of Plaintiff's and Class Members' Personal Information with full awareness of both the likelihood of a cyberattack targeted to acquire that information and the severe consequences that would result to Plaintiff and Class Members if the confidentiality of the Personal Information was breached, Defendant assumed a special relationship that required it to guard against the foreseeable conduct of a criminal third party. If Defendant had not intervened by taking charge of Plaintiff's and Class Member's Personal Information, no harm would have resulted to Plaintiff and Class Members as a result of the Data Breach.

127. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Personal Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Personal Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's and its third-party application's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information.

128. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members 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.

129. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Personal Information, which remains in Defendant's and its third-party application's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information in its continued possession.

130. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

131. Defendant's negligent conduct is ongoing, in that it still holds the Personal Information of Plaintiff and Class Members in an unsafe and insecure manner.

132. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to: (i) strengthen its and its third-party applications' data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND CAUSE OF ACTION
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and Class Members)

133. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

134. Defendant entered into a written contract with its third-party application to provide certain services for which Defendant's third-party application required Plaintiff's and Class Members' Personal Information.

135. In exchange, on information and belief, Defendant and its third-party application agreed, in part, to implement adequate security measures to safeguard the Personal

Information of Plaintiff and Class Members and to timely and adequately notify them of the Data Breach.

136. These contracts were made expressly for the benefit of Plaintiff and Class Members, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its third-party application.

137. Defendant and/or its third-party application breached the contract it entered into by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's Personal Information from unauthorized disclosure to third parties, (iii) failing to perform due diligence and to verify, audit, or monitor the integrity of third party networks on which it shared Personal Information, and (iv) failing to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

138. Plaintiff and Class Members were harmed by Defendant's breach of its contracts with its third-party application, its third-party application's breach of its contract with Defendant, or both, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and Class Members)

139. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

140. Plaintiff and the Class entrusted their Personal Information with Defendant. In doing so, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached, compromised, or stolen.

141. The statements in Defendant's Privacy Policy described herein support the existence of an implied contract.

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

143. Defendant breached the implied contract with Plaintiff and the Class by failing to safeguard and protect their Personal Information, by failing to delete the Personal Information of Plaintiff and the Class once their relationship ended, and by failing to provide timely and accurate notice to them that the Personal Information was compromised as a result of the Data Breach.

144. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered, and will continue to suffer, ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss an economic harm; actual identify 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 time that the Plaintiff and Class have not been compensated for.

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

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and Class Members)

146. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

147. Plaintiff and Class Members, including both customers and employees of Defendant, conferred a monetary benefit on Defendant.

148. Specifically, customers paid for services offered by the Defendant and/or its agents, while employees contributed their labor. In both instances, they provided the Defendant with their Personal Information. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Personal Information protected with adequate data security.

149. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Personal Information entrusted to it. Defendant profited from Plaintiff's and Class Members' retained data and used Plaintiff's and Class Members' Personal Information for business purposes.

150. Defendant failed to secure Plaintiff's and Class Members' Personal Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Personal Information provided.

151. Defendant acquired the Personal Information through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

152. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Personal Information, they would not have entrusted their Personal Information with Defendant or obtained services at Defendant.

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

154. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

155. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Personal Information; (iii) lost time and opportunity

costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Personal Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information.

156. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

157. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

FIFTH CAUSE OF ACTION
California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff and Class Members)

158. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

159. Defendant's acts and omissions as alleged herein emanated and directed from California.

160. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

161. Defendant stored the Personal Information of Plaintiff and Class Members in its computer systems.

162. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations that would have kept Plaintiff's and Class Members' Personal Information secure and prevented the loss or misuse of that Personal Information.

163. Defendant did not disclose at any time that Plaintiff's and Class Members' Personal Information was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only one in possession of that material information, which Defendant had a duty to disclose.

Unlawful Business Practices

164. As noted above, Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, by omission, the safety of its computer systems, specifically the security thereof, and its ability to safely store Plaintiff's and Class Members' Personal Information.

165. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security.

166. If Defendant had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiff and Class Members of the Data Breach.

167. Defendant's acts and omissions as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the FTC Act.

168. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, Plaintiff's and Class Members' Personal Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out of pocket losses

for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Unfair Business Practices

169. Defendant engaged in unfair business practices under the "balancing test." The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweighs any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and failure to disclose inadequacies of Defendant's data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiff and Class Members, directly causing the harms alleged below.

170. Defendant engaged in unfair business practices under the "tethering test." Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See*, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

171. Defendant engaged in unfair business practices under the "FTC test." The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects hundreds of thousands of Class Members and has caused those persons to suffer actual harm. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and Class Members' Personal Information to third parties without their consent, diminution in value of their Personal Information, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses

or protective measures. This harm continues given the fact that Plaintiff's and Class Members' Personal Information remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g., In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated §5(a) of FTC Act).

172. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. Plaintiff's and Class Members' Personal Information was taken and in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

173. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, Plaintiff and Class Members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent Class Members;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members'

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

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

D. For injunctive relief requested by Plaintiff, 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 Defendant from engaging in the wrongful and unlawful acts described herein;

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

iii. Requiring Defendant to delete, destroy, and purge the Personal Information of Plaintiff and Class Members unless Defendant 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 Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Personal Information of Plaintiff and Class Members;

v. Requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information for Plaintiff's and Class Members' respective lifetimes;

vi. Prohibiting Defendant from maintaining the Personal Information of Plaintiff and Class Members on a cloud-based database;

vii. Requiring Defendant 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 its and its third-party application's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of its network is compromised, hackers cannot gain access to other portions of its systems;

xi. Requiring Defendant to conduct regular database scanning and securing checks;

xii. Requiring Defendant 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 Information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xiii. Requiring Defendant 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;

xiv. Requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with its policies, programs, and systems for protecting Personal Information;

xv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor its information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. Requiring Defendant 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;

xvii. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from its servers; and

xviii. 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 Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for Class Members, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than a lifetime of credit monitoring services for Plaintiff and Class Members;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: February 29, 2024

Respectfully Submitted,

/s/ *Byron T. Ball*

Byron T. Ball (SBN 150195)
THE BALL LAW FIRM APC
100 Wilshire Blvd. Suite 700
Santa Monica, California 90401
Telephone: (310) 980-8039
Email: btb@balllawllp.com

/s/ William B. Federman

*William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
P: (405) 235-1560
F: (405) 239-2112
wbf@federmanlaw.com

Attorneys for Plaintiff and the Proposed Class
**Pro Hac Vice forthcoming*