William B. Federman
(admitted *pro hac vice*)
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
-and-
212 W. Spring Valley Road
Richardson, Texas 75081

Interim Co-Lead Counsel for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

AMANDA PEREZ, SASHA LIPP, JAMES MURRAY, MICHAEL HALPREN AND ELIJAH JOHNSON, on behalf of themselves and all others similarly situated, Plaintiffs, v. **CARVIN WILSON SOFTWARE, LLC d/b/a CARVIN SOFTWARE, LLC,** Defendant.	Case No. 2:23-cv-00792-SMM **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Amanda Perez, Sasha Lipp, James Murray, Michael Halpren and Elijah Johnson ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Carvin Wilson Software, LLC d/b/a Carvin Software, LLC ("Carvin Software" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against Carvin Software for its failure to properly secure and safeguard Plaintiffs' and other similarly situated individuals' names, Social Security numbers and financial account information (the "PII" or "Personal Information") from unauthorized access and disclosure.

2. Defendant, based in Gilbert, Arizona, is a staffing software solutions and consulting services company. As part of its business, and in order to earn profits, Defendant obtained and stored the PII of Plaintiffs and Class Members.

3. On March 9, 2023, Carvin Software identified unusual activity on certain systems within its computer network. Following an investigation, Carvin Software determined that certain files containing the sensitive Personal Information of Plaintiffs and "Class Members" (defined below) were copied from its network without authorization between February 22, 2023 and March 9, 2023 (the "Data Breach" or "Breach").

4. According to Carvin Software, the Personal Information exfiltrated by cybercriminals includes names, Social Security numbers and financial account information[1] of 356,871 individuals.[2]

5. As a result of Defendant's inability to timely detect the Data Breach, Plaintiffs and Class Members had no idea for *weeks* that their PII had been compromised, and that they were at significant risk of experiencing identity theft and various other forms of personal, social, and financial harm. This substantial and imminent risk will remain for their respective lifetimes.

6. The PII compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, names, Social Security numbers and financial account information that Carvin Software collected from Plaintiffs' and Class Members' employers and maintained within its systems.

7. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in

---

[1] *See Carvin Software, LLC*, WASHINGTON STATE OFFICE OF THE ATTORNEY GENERAL, https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachA22964.pdf (last visited Aug. 3, 2023).

[2] Data Breach Notifications, *Carvin Software, LLC*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/b7cc5af8-f194-4183-a204-c317f8f66703.shtml (last visited Aug. 3, 2023).

Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. There has been no assurance offered by Defendant that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

9. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their PII, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiffs bring this class action lawsuit to address Carvin Software's inadequate safeguarding of Class Members' PII that it collected and maintained, and its failure to timely detect the Data Breach.

11. The potential for improper disclosure and theft of Plaintiffs' and Class Members' PII was a known risk to Carvin Software and, thus, it was on notice that failing to take necessary steps to secure the PII left it vulnerable to an attack.

12. Upon information and belief, Carvin Software and its employees failed to properly monitor its systems and implement adequate data security practices with regard to such systems that housed the PII. Had Carvin Software properly monitored its network systems and implemented such practices, it could have prevented the Data Breach or at least discovered it sooner.

13. Plaintiffs' and Class Members' identities are now at risk because of Carvin Software's negligent conduct because the PII that Carvin Software collected and maintained is now in the hands of data thieves and other unauthorized third parties.

14. Plaintiffs seek to remedy these harms on behalf of themselves and all other similarly situated individuals whose PII was accessed and/or compromised during the Data Breach.

II. PARTIES

15. Plaintiff **Amanda Perez**, is, and at all times mentioned herein was, an individual citizen of the State of Maine.

16. Plaintiff **Sasha Lipp**, is, and at all times mentioned herein was, an individual citizen of the State of California.

17. Plaintiff **James Murray**, is, and at all times mentioned herein was, an individual citizen of the State of California.

18. Plaintiff **Michael Halpren**, is, and at all times mentioned herein was, an individual citizen of the State of California.

19. Plaintiff **Elijah Johnson**, is, and at all times mentioned herein was, an individual citizen of the State of Tennessee.

20. Defendant **Carvin Wilson Software, LLC d/b/a Carvin Software, LLC** is a limited liability company with its principal place of business at 70 South Val Vista Drive, Suite A3, Gilbert, AZ 85296 in Maricopa County.

III. JURISDICTION AND VENUE

21. The 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 $5,000,000, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Carvin Software, including each Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

22. This Court has jurisdiction over Carvin Software because Carvin Software operates in and/or is incorporated in this District.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Carvin Software has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Carvin Software's Business and Collection of Plaintiffs' and Class Members' PII.

24. Carvin Software is a software and consulting services company.

25. Founded in 2004, Carvin Software specializes in providing software solutions to staffing companies nationwide in both front-office and back-office functions, such as payroll, billing, and accounting. Carvin Software employs more than 25 people.[3]

26. As a condition of providing services, Carvin Software requires that its customers entrust it with highly sensitive PII.

---

[3] *See Carvin Software*, TRACXN, https://tracxn.com/d/companies/carvin-software/__p0embk4OZ-xhVdIK7ID1qr40pgw2_anfJ0YStgQxMNM (last visited August 3, 2023).

27. Because of the highly sensitive and personal nature of the information Carvin Software acquires and stores with respect to its customers' current and former employees (collectively referred to herein as "employees"), Carvin Software, upon information and belief, promises to, among other things: keep its customers' employees' PII private; comply with industry standards related to data security and the maintenance of its customers' employees' PII; inform its customers (and their employees) of its legal duties relating to data security and comply with all federal and state laws protecting its customers' employees' PII; only use and release its customers' employees' PII for reasons that relate to the services it provides; and provide adequate notice to its customers' employees if their PII is disclosed without authorization.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Carvin Software assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure and exfiltration.

29. Plaintiffs and Class Members and their respective employers relied on Carvin Software to keep their PII confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. <u>The Data Breach and Carvin Software's Inadequate Notice.</u>

30. Between, at least, February 22, 2023, and March 9, 2023, third-party cybercriminals conducted a successful cybersecurity attack whereby they infiltrated

Defendant's systems and gained unauthorized access to the Personal Information of hundreds of thousands of individuals whose data was stored within Defendant's systems.[4]

31. The Breach was not detected until March 9, 2023.[5] Prior to that time, unauthorized cybercriminals were able to roam Defendant's systems for weeks without detection or interference.

32. Following a forensic investigation, it was determined that the cybercriminals accessed and copied files containing a cache of highly sensitive PII, including Plaintiffs' and Class Members' names, Social Security numbers and financial account information.[6]

33. On or about May 2, 2023, Carvin Software finally began to notify its customers' employees' that their PII was compromised.

34. Carvin Software delivered the Notice to Plaintiffs and Class Members, alerting them that their highly sensitive PII had been exposed in an "incident."

35. The Notice then attached some pages entitled "Steps You Can Take to Help Protect Personal Information," which listed time-consuming steps that victims of data security incidents can take to mitigate the inevitable negative impacts of the Data Breach on their lives, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. In fact, Carvin "encourage[d]" breach victims "to

---

[4] *See Carvin Software, LLC*, WASHINGTON STATE OFFICE OF THE ATTORNEY GENERAL, https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachA22964.pdf (last visited Aug. 3, 2023).

[5] *Id.*

[6] *Id.*

remain vigilant against potential incidents of identity theft and fraud," acknowledging that Plaintiffs and Class Members are at significant risk of harm.

36. Other than providing one year of crediting monitoring that Plaintiffs and Class Members would have to affirmatively sign up for (and which offer has already expired), Carvin Software offered no other substantive steps to help victims like Plaintiffs and Class Members to protect themselves. On information and belief, Carvin Software sent a similar generic letter to all individuals affected by the Data Breach.

37. Carvin Software had obligations created by contract, industry standards, and common law to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

38. Plaintiffs and Class Members provided their PII to their employers – Carvin Software's clients – with the reasonable expectation and mutual understanding that Carvin Software would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

39. Carvin Software's data security obligations were particularly important given the substantial increase in cyberattacks in recent years. Carvin Software knew or should have known that its electronic records would be targeted by cybercriminals. However, even with these obligations and this knowledge, it failed to safeguard the PII.

C. Carvin Software Failed to Comply with FTC Guidelines

40. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all

business decision-making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

41. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

42. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

43. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ

reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

44. As evidenced by the Data Breach, Carvin Software failed to properly implement basic data security practices. Carvin Software's failure to employ reasonable and appropriate measures to protect against unauthorized access to and exfiltration of Plaintiffs' and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

45. Carvin Software was at all times fully aware of its obligation to protect the PII of its customers' employees yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Carvin Software Failed to Comply with Industry Standards

46. As noted above, experts studying cybersecurity routinely identify businesses like Carvin Software as being particularly vulnerable to cyberattacks because of the value of employee PII which they collect and maintain.

47. Some industry best practices that should be implemented by businesses like Carvin Software include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

48. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

49. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8 and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

50. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. Carvin Software Breached its Duty to Safeguard Plaintiffs' and Class Members' PII

51. In addition to its obligations under federal and state law, Carvin Software owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. Carvin Software owed a duty to Plaintiffs and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and

ensuring that its computer systems, networks and protocols adequately protected the PII of Plaintiffs and Class Members.

52. Carvin Software breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Carvin Software's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect its customers' employees' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers' employees' PII;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' PII.

53. Carvin Software negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII by allowing cyberthieves to access its computer network and

systems which contained unsecured and unencrypted PII and then subsequently copy such PII therefrom.

54. Had Carvin Software remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

55. Accordingly, Plaintiffs' and Class Members' lives have been severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft.

F. Carvin Software Should Have Known that Cybercriminals Target Highly Sensitive PII to Carry Out Fraud and Identity Theft

56. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[7] Exposure of highly sensitive personal information that an individual wishes to keep private may cause harm to that individual, such as the ability to obtain or keep employment.

[7] *FTC Informational Injury Workshop: BE and BCP Staff Perspective*, FEDERAL TRADE COMMISSION, (October 2018), *available at* https://www.ftc.gov/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective (last visited Aug. 3, 2023).

57. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

58. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

59. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

60. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' PII to access

accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

61. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps (similar to those suggested by Defendant in its Notice) to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[8] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

62. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[8] *See IdentityTheft.gov,* FEDERAL TRADE COMMISSION, *available at* https://www.identitytheft.gov/Steps (last visited Aug. 3, 2023).

63. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

64. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[9] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

65. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a

[9] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. DEP'T OF JUSTICE (Feb. 10, 2020), *available at* https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited Aug. 3, 2023).

[10] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Aug. 3, 2023).

term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[11]

66. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[12]

[11] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Aug. 3, 2023).

[12] *See Dark Web Price Index: The Cost of Email Data*, MAGICSPAM (Sept. 12, 2022), https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited Aug. 3, 2023).

67. The Dark Web Price Index of 2022, published by PrivacyAffairs[13] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

68. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

69. Likewise, the value of PII is increasingly evident in our digital economy. Many companies collect PII for the purposes of data analytics and marketing. These companies, collect it to better target customers and share it with third parties for similar purposes.[14]

[13] *See* Patricia Ruffio, *Dark Web Price Index 2022*, PRIVACY AFFAIRS (June 10, 2023), https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited Aug. 3, 2023).

[14] *See* Robinhood Privacy Policy, ROBINHOOD (May 17, 2023), https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited Aug. 3, 2023).

70. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[15]

71. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather in the economic benefit consumers derive from being able to use it and control the use of it.

72. PII is a valuable property right.[16] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

73. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[17]

---

[15] *See* John T. Soma, *et al.*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J. L. & Tech. 11, 14 (2009) *available at* https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1310&context=jolt (last visited Aug. 3, 2023).

[16] *See, e.g., id.* at 3–4 ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[17] David Lazarus, Shadowy data brokers make the most of their invisibility cloak, LOS ANGELES TIMES (Nov. 5, 2019, 5:00 AM PT), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Aug. 3, 2023).

74. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[18]

75. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[19]

76. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

77. Data breaches, like the one at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

78. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property,

[18] DATACOUP, https://datacoup.com/ (last visited Aug. 3, 2023).

[19] Computer & Mobile Panel, *Frequently Asked Questions*, NIELSEN, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Aug. 3, 2023).

resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

79. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[20]

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

80. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

81. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. <u>Common Injuries and Damages</u>

82. Plaintiffs and Class Members have been damaged by the compromise of their PII in the Data Breach.

[20] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited Aug. 3, 2023).

83. Plaintiffs and Class Members entrusted their PII to Defendant through their respective employers in order to receive employment and benefit from Defendant's staffing solution services.

84. Plaintiffs' PII was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

85. As a direct and proximate result of Carvin Software's actions and omissions, Plaintiffs and Class Members have been harmed and/or are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names and other forms of identity theft.

86. Further, as a direct and proximate result of Carvin Software's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

87. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion and other illegal schemes through the misuse of their PII, since potential fraudsters will likely use such PII to carry out such targeted schemes against Plaintiffs and Class Members.

88. The PII maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which have already been used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

89. Additionally, Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and records for misuse.

90. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach 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. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Placing "freezes" and "alerts" with credit reporting agencies;

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

f. Contacting financial institutions and closing or modifying financial accounts;

g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

h. 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

i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

91. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to still be in the possession of Carvin Software, is protected

from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

92. As a direct and proximate result of Carvin Software's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth herein.

H. Plaintiffs' Experiences

Plaintiff Amanda Perez

93. Plaintiff Perez provided her sensitive PII to one of the entities that contracts with Defendant. Upon information and belief, Defendant thereafter acquired this PII and used this information when providing software and services relating to consulting, payroll, or billing.

94. Plaintiff Perez received a letter, dated May 2, 2023, from Defendant notifying her of the Data Breach. The letter advised that unauthorized third parties had accessed and copied files on Defendant's network. The letter further advised that Plaintiff Perez's PII—including her name, Social Security number and financial account information—was identified as having been within the files that were compromised and copied by unauthorized third parties during the Data Breach.

95. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Perez faces, the letter offered Plaintiff Perez a temporary subscription to credit

monitoring services. The letter further instructed Plaintiff Perez to "remain vigilant against potential incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors." The letter additionally encouraged Plaintiff Perez to consider implementing the protective measures detailed in the "'Steps You Can Take to Help Protect Personal Information' section of [the] letter."

96. As a result of the Data Breach, Plaintiff Perez has spent several hours investigating the Data Breach, researching how best to ensure that she is protected from identity theft, reviewing account statements and other information, changing her bank account information, and taking other steps in an attempt to mitigate the harm caused by the Data Breach. This is valuable time Plaintiff Perez spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

97. Plaintiff Perez greatly values her privacy and is very careful with her PII. Plaintiff Perez stores any documents containing PII in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Perez has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Moreover, Plaintiff Perez diligently chooses unique usernames and passwords for her various online accounts. When Plaintiff Perez does entrust a third-party with her PII, it is only because she understands such information will be reasonably safeguarded from foreseeable threats, and that she will be timely notified if her data is exposed.

98. The Data Breach caused Plaintiff Perez to suffer a loss of privacy.

99. As a result of the Data Breach, Plaintiff Perez will face a substantial risk of imminent harm for the rest of her life.

100. Plaintiff Perez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

101. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff Perez to suffer fear, anxiety, annoyance, inconvenience and nuisance.

102. The Data Breach caused Plaintiff Perez to suffer a diminution in the value of her PII.

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

104. As a result of the Data Breach, Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's PII that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of time and effort that Plaintiff Perez has had to expend in an attempt to ameliorate, mitigate and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (e) continued risk to Plaintiff's PII, which remains in the possession of Defendant and

which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Sasha Lipp

105. Plaintiff Sasha Lipp provided her sensitive PII to Pirate Staffing, which was an entity who contracted with Defendant for software services. Upon information and belief, Defendant acquired Plaintiff Sasha Lipp's PII from Pirate Staffing and used that PII when providing software and services relating to consulting, payroll, or billing.

106. Plaintiff Sasha Lipp received a letter, dated May 2, 2023, from Defendant notifying her of the Data Breach. The letter advised that unauthorized third parties had accessed and copied files on Defendant's network. The letter further advised that Plaintiff Sasha Lipp's PII—including her name and Social Security Number—was identified as having been within the files that were compromised and copied by unauthorized third parties during the Data Breach.

107. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Sasha Lipp faces, the letter offered Plaintiff a 12-month subscription to credit monitoring services. The letter further instructed Plaintiff Sasha Lipp to "remain vigilant against potential incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors." The letter additionally encouraged Plaintiff Sasha Lipp to consider implementing the protective measures detailed in the "'Steps You Can Take to Help Protect Personal Information' section of [the] letter."

108. As a result of the Data Breach, Plaintiff Sasha Lipp has spent approximately 35–40 hours researching the Data Breach, verifying the legitimacy of the notice letter, researching various credit monitoring services, reviewing her bank accounts, making telephone calls to her banks and credit card companies related to the breach, monitoring her credit report, changing her passwords and payment account numbers, and other necessary mitigation efforts. This is valuable time Plaintiff Sasha Lipp spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

109. Over the last several months, Plaintiff Sasha Lipp has experienced a significant increase in spam e-mail, texts, mail and phone calls from unknown sources. Additionally, Plaintiff Sasha Lipp has experienced at least two unauthorized charges to her Bank of America account over the several weeks prior to this filing of this Complaint. She has contacted Bank of America and an investigation regarding those charges is currently being conducted.

110. Plaintiff Sasha Lipp greatly values her privacy and is very careful with her PII. Plaintiff Sasha Lipp stores any documents containing PII in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Sasha Lipp has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Moreover, Plaintiff Sasha Lipp diligently chooses unique usernames and passwords for her various online accounts. When Plaintiff Sasha Lipp does entrust a third-party with her PII, it is only because she understands such information will be reasonably safeguarded from foreseeable threats, and that she will be timely notified if her data is exposed.

111. The Data Breach caused Plaintiff Sasha Lipp to suffer a loss of privacy.

112. As a result of the Data Breach, Plaintiff Sasha Lipp will face a substantial risk of imminent harm for the rest of her life.

113. Plaintiff Sasha Lipp anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

114. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff Sasha Lipp to suffer fear, anxiety, annoyance, inconvenience and nuisance.

115. The Data Breach caused Plaintiff Sasha Lipp to suffer a diminution in the value of her PII.

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

117. As a result of the Data Breach, Plaintiff Lipp has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's PII that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of time and effort that Plaintiff Sasha Lipp has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (e) continued risk to Plaintiff's PII, which remains in the

possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff James Murray

118. Plaintiff Murray provided his sensitive PII to one of the entities that contracts with Defendant. Upon information and belief, Defendant thereafter acquired this PII and used this information when providing software and services relating to consulting, payroll, or billing.

119. Plaintiff Murray received a letter, dated May 2, 2023, from Defendant notifying him of the Data Breach. The letter advised that unauthorized third parties had accessed and copied files on Defendant's network. The letter further advised that Plaintiff Murray's PII—including his name, Social Security number and financial account information—was identified as having been within the files that were compromised and copied by unauthorized third parties during the Data Breach.

120. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Murray faces, the letter offered Plaintiff Murray a temporary subscription to credit monitoring services. The letter further instructed Plaintiff Murray to "remain vigilant against potential incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors." The letter additionally encouraged Plaintiff Murray to consider implementing the protective measures detailed in the "'Steps You Can Take to Help Protect Personal Information' section of [the] letter."

121. As a result of the Data Breach, Plaintiff Murray has spent numerous hours, he estimates in excess of 25 hours, researching the Data Breach, verifying the legitimacy of the notice letter, signing up for increased credit monitoring and identity theft protection services, reviewing his bank accounts, monitoring his credit reports, checking his credit score, changing his passwords and payment account numbers, carefully reviewing and filtering through suspicious emails, texts and calls, reviewing notifications from his identity theft protection services, and taking other steps in an attempt to mitigate the harm caused by the Data Breach. This is valuable time Plaintiff Murray spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

122. Indeed, Plaintiff Murray now pays out-of-pocket for credit monitoring and identity theft protection services through MyFico at a cost of more than $30 a month.

123. Through these paid MyFico services, Plaintiff Murray has already received notifications that his information was located on the dark web in April and May 2023.

124. Plaintiff Murray greatly values his privacy and is very careful with his PII. Plaintiff Murray stores any documents containing PII in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Murray has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Moreover, Plaintiff Murray diligently chooses unique usernames and passwords for his various online accounts. When Plaintiff Murray does entrust a third-party with his PII, it is only because he understands such information will be reasonably safeguarded from foreseeable threats, and that he will be timely notified if his data is exposed.

125. The Data Breach caused Plaintiff Murray to suffer a loss of privacy.

126. As a result of the Data Breach, Plaintiff Murray will face a substantial risk of imminent harm for the rest of his life.

127. Plaintiff Murray anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

128. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff Murray to suffer fear, anxiety, annoyance, inconvenience and nuisance.

129. The Data Breach caused Plaintiff Murray to suffer a diminution in the value of his PII.

130. Plaintiff Murray has a continuing interest in ensuring that his PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

131. As a result of the Data Breach, Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's PII that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of time, effort, and money that Plaintiff Murray has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (e) continued risk to Plaintiff's PII, which remains in the possession of

Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Michael Halpren

132. Plaintiff Halpren is unsure how Carvin Software came into possession of his Personal Information but assumes a staffing company receiving its software and financial accounting services from Carvin Software provided Defendant with his PII, including but not limited to, his name, Social Security Number, and financial information.

133. Plaintiff Halpren received a letter, dated May 2, 2023, from Defendant notifying him of the Data Breach. The letter advised that unauthorized third parties had accessed and copied files on Defendant's network. The letter further advised that Plaintiff Halpren's PII—including his name, Social Security number and financial account information—was identified as having been within the files that were compromised and copied by unauthorized third parties during the Data Breach.

134. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Halpren faces, the letter offered Plaintiff Halpren a temporary subscription to credit monitoring services. The letter further instructed Plaintiff Halpren to "remain vigilant against potential incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors." The letter additionally encouraged Plaintiff Halpren to consider implementing the protective measures detailed in the "'Steps You Can Take to Help Protect Personal Information' section of [the] letter."

135. As a result of the Data Breach, Plaintiff Halpren has spent significant time on activities including verifying the legitimacy of the Breach Notice; self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred; and other necessary mitigation efforts. This is valuable time Plaintiff Halpren spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

136. Following the Data Breach, Plaintiff was notified by his bank regarding a fraudulent attempt to use his Apple Pay account to make a purchase. This demonstrates that Plaintiff's information was stolen in the Data Breach and has been placed in the hands of cybercriminals.

137. Plaintiff Halpren greatly values his privacy and is very careful with his PII. Plaintiff Halpren stores any documents containing PII in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Halpren has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Moreover, Plaintiff Halpren diligently chooses unique usernames and passwords for his various online accounts. When Plaintiff Halpren did entrust a third-party with his PII, it is only because he understands such information will be reasonably safeguarded from foreseeable threats, and that he will be timely notified if his data is exposed.

138. The Data Breach caused Plaintiff Halpren to suffer a loss of privacy.

139. As a result of the Data Breach, Plaintiff Halpren will face a substantial risk of imminent harm for the rest of his life.

140. Plaintiff Halpren anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

141. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff Halpren to suffer fear, anxiety, annoyance, inconvenience and nuisance.

142. The Data Breach caused Plaintiff Halpren to suffer a diminution in the value of his PII.

143. Plaintiff Halpren has a continuing interest in ensuring that his PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

144. As a result of the Data Breach, Plaintiff Halpren has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's PII that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of time and effort that Plaintiff Halpren has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (e) continued risk to Plaintiff's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Elijah Johnson

145. Plaintiff Johnson provided his sensitive PII to Labor Exchange for temporary employment. Labor Exchange is one of many entities that contracts with Defendant. Upon information and belief, Defendant thereafter acquired his PII and used it when providing software and services to Labor Exchange relating to consulting, payroll and/or billing.

146. Plaintiff Johnson received a letter, dated May 2, 2023, from Defendant notifying him of the Data Breach. The letter advised that unauthorized third parties had accessed and copied files on Defendant's network. The letter further advised that Plaintiff Johnson's PII—including his name and Social Security number—was identified as having been within the files that were compromised and copied by unauthorized third parties during the Data Breach.

147. Recognizing the present, immediate and substantially increased risk of harm Plaintiff Johnson faces, the letter offered Plaintiff Johnson a 12-month subscription to credit monitoring services. The letter further instructed Plaintiff Johnson to "remain vigilant against potential incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors." The letter additionally encouraged Plaintiff Johnson to consider implementing the protective measures detailed in the "'Steps You Can Take to Help Protect Personal Information' section of [the] letter."

148. As a result of the Data Breach, Plaintiff Johnson has spent approximately 48 hours researching the Data Breach, verifying the legitimacy of the notice letter, signing up for the credit monitoring service, reviewing his bank accounts, monitoring his credit report,

filtering through hundreds of spam texts, calls and emails, and other necessary mitigation efforts. This is valuable time Plaintiff Johnson spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

149. Specifically, Plaintiff Johnson began to receive dozens of harassing, targeted phishing texts, emails and phone calls a week, with such harassment beginning just days after he received the Notice from Defendant.

150. Plaintiff Johnson greatly values his privacy and is very careful with his PII. Plaintiff Johnson stores any documents containing PII in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Johnson has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. When Plaintiff Johnson does entrust a third-party with his PII, it is only because he understands such information will be reasonably safeguarded from foreseeable threats, and that he will be timely notified if his data is exposed.

151. The Data Breach caused Plaintiff Johnson to suffer a loss of privacy.

152. As a result of the Data Breach, Plaintiff Johnson will face a substantial risk of imminent harm for the rest of his life.

153. Plaintiff Johnson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

154. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff Johnson to suffer fear, anxiety, annoyance, inconvenience and nuisance,

especially knowing now, as a young student, that his PII is in the hands of cybercriminals and being misused to engage in targeted phishing schemes against him.

155. The Data Breach caused Plaintiff Johnson to suffer a diminution in the value of his PII.

156. Plaintiff Johnson has a continuing interest in ensuring that his PII, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

157. As a result of the Data Breach, Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's PII that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of time and effort that Plaintiff Johnson has had to expend in an attempt to ameliorate, mitigate and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (e) continued risk to Plaintiff's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

V. CLASS ACTION ALLEGATIONS

158. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure.

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

> All individuals in the United States whose PII was accessed without authorization in the Carvin Software Data Breach, including all those who received a notice of the Data Breach (the "Nationwide Class" or "Class").

160. The **California Subclass** that Plaintiffs Lipp, Murray and Halpren seek to represent is defined as follows:

> All individuals in the State of California whose PII was accessed without authorization in the Carvin Software Data Breach, including all those who received a notice of the Data Breach (the "California Subclass").

161. The **Tennessee Subclass** that Plaintiff Johnson seeks to represent is defined as follows:

> All individuals in the State of Tennessee whose PII was accessed without authorization in the Carvin Software Data Breach, including all those who received a notice of the Data Breach (the "Tennessee Subclass").

162. Excluded from the Class—which includes the Nationwide Class and the Subclasses—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; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

163. Plaintiffs reserve the right to modify or amend the definition of the proposed class and/or subclasses before the Court determines whether certification is appropriate.

164. Numerosity, Fed R. Civ. P. 23(a)(1): Plaintiffs are representatives of the proposed Class, consisting of 356,871 members – far too many to join in a single action.

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

a. Whether Carvin Software had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII;

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

c. Whether Carvin Software was negligent in maintaining, protecting and securing PII;

d. Whether Carvin Software took reasonable measures to determine the extent of the Data Breach after discovering it;

e. Whether Carvin Software's Breach Notice was reasonable;

f. Whether the Data Breach caused Plaintiffs and the Class injuries;

g. What the proper damages measure is;

h. Whether Carvin Software violated the statutes alleged in this Complaint; and

i. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

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

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

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

169. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class

Members to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like 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.

170. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs 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 Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

171. 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 demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

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

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

FIRST CAUSE OF ACTION
Negligence
(On behalf of Plaintiffs and the Class)

175. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

176. Carvin Software required Plaintiffs and Class Members to submit non-public PII to it in its ordinary course of business.

177. By collecting and storing this data in its computer system and network for its own commercial gain, Carvin Software owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' PII held within it—to prevent disclosure of the PII, and to safeguard it from theft. Carvin Software's duty included a responsibility to implement processes that would allow it to detect a breach of

its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

178. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Carvin Software holds vast amounts of PII, it was inevitable that unauthorized individuals would, at some point, try to access Carvin Software's databases of PII and attempt to acquire that PII for its value.

179. After all, PII is highly valuable, and Carvin Software knew, or should have known, the risk in obtaining, using, handling, emailing and storing the PII of Plaintiffs and Class Members. Thus, Carvin Software knew, or should have known, the importance of exercising reasonable care in handling the PII entrusted to it.

180. Carvin Software owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

181. Carvin Software's duty of care to use reasonable security measures arose because of the special relationship that existed between Carvin Software, Plaintiffs and Class Members, which is recognized by various laws and regulations, as detailed herein. That special relationship arose because Carvin Software was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach. Plaintiffs and Class Members had no way of influencing Defendant's data policies or of verifying the integrity of Defendant's computer systems.

182. Under the FTCA, Carvin Software had a duty to employ reasonable security measures. Specifically, this statute 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.[21]

183. Moreover, Plaintiffs' and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Defendant inflicted upon Plaintiffs and Class Members.

184. Additionally, under the Arizona Data Breach Notification Act, Carvin Software has a duty to promptly notify affected persons of a data breach so that they can take action to protect themselves. Specifically, if "the investigation [of a potential data breach] results in a determination that there has been a security system breach, the person that owns or licenses the computerized data, within forty-five days after the determination, shall . . . [n]otify the individuals affected."[22]

185. Moreover, Plaintiffs' and Class Members' injuries are precisely the type of injuries that the Arizona Data Breach Notification Act guards against.

186. Carvin Software's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Carvin Software is bound by industry standards to protect confidential PII.

---

[21] 15 U.S.C. §45.
[22] A.R.S §§18-551, 18-552.

187. Carvin Software owed Plaintiffs and members of the Class a duty to notify them within a reasonable time frame of any breach to their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiffs and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of Carvin Software's Data Breach.

188. Carvin Software owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Carvin Software knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Carvin Software actively sought and obtained the PII of Plaintiffs and Class Members.

189. Carvin Software breached its duties and, thus, was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII. And, but for Carvin Software's negligence, Plaintiffs and Class Members would not have been injured. The specific negligent acts and omissions committed by Carvin Software include, but are not limited to:

a. Failing to adopt, implement and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to comply with—and thus violating—the FTCA and its regulations;

c. Failing to comply with—and thus violating—the Arizona Data Breach Notification Act and its regulations;

d. Failing to adequately monitor the security of its network and systems;

f. Failing to have in place data breach mitigation policies and procedures;

g. Allowing unauthorized access to Class Members' PII;

h. Failing to detect in a timely manner that Class Members' PII had been compromised; and

i. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

190. It was foreseeable that Carvin Software's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in this industry. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

191. Simply put, Carvin Software's negligence actually and proximately caused Plaintiffs' and Class Members' actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their PII by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Carvin Software's negligence. Moreover, injuries-in-fact and damages are ongoing, imminent and immediate.

192. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

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

193. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

194. Carvin Software entered into various contracts with its financial and staffing clients to provide software, payroll and other services. As a material part of those contracts Defendant agreed to implement reasonable data security practices and procedures sufficient to safeguard the PII provided to it by its clients – namely, the PII belonging to its clients' employees, including Plaintiffs and Class Members.

195. These contracts are virtually identical to each other and the provisions regarding PII were made expressly for the benefit of Plaintiffs and the Class, as it was their confidential Personal Information that Carvin Software agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiffs and the Class were the direct and primary objective of the contracting parties.

196. Carvin Software knew that if it were to breach these contracts with its staffing and financial clients, Plaintiffs and the Class would be harmed by, among other things, fraudulent misuse of their PII.

197. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiffs' and Class Members' PII.

198. As a reasonably foreseeable result of the Data Breach, Plaintiffs and the Class were harmed by Carvin Software's failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm sustained from the loss of their PII to cybercriminals.

199. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On behalf of Plaintiffs and the Class)

200. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

201. This claim is pleaded in the alternative to the third-party beneficiary breach of contract claim above (Count II).

202. Plaintiffs and Class Members conferred a benefit on Carvin Software in the form of highly valuable PII necessary for Carvin Software to render certain services to its clients, for which services Carvin Software received monetary payments. A portion of this benefit was to have been used by Carvin Software for data security measures to secure Plaintiffs' and Class Members' valuable PII.

203. Carvin Software enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Carvin Software chose to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class

Members, on the other hand, suffered as a direct and proximate result of Carvin Software's failure to provide adequate security.

204. Under the principles of equity and good conscience, Carvin Software should not be permitted to retain the full value of its profits resulting from its collection and storage of the Plaintiffs' and Class Members' PII, because Carvin Software failed to implement appropriate data management and security measures that are mandated by industry standards.

205. If Plaintiffs and Class Members knew that Carvin Software had not secured their PII, they would not have agreed to disclose their data to Carvin Software's clients.

206. Plaintiffs and Class Members have no adequate remedy at law.

207. As a direct and proximate result of Carvin Software's conduct, Plaintiffs and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their PII is used; (3) the compromise, publication and/or theft of their PII; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft; (6) the continued risk to their PII, which remain in Carvin Software's possession and are subject to further unauthorized disclosures so long as Carvin Software fails to undertake appropriate and adequate measures to protect the PII in its possession; and, (7) future expenditures of time,

effort and money that will be spent trying to prevent, detect, contest, and repair the impact of Carvin Software's Data Breach.

208. As a direct and proximate result of Carvin Software's conduct, Plaintiffs and Class Members suffered—and will continue to suffer—other forms of injury and/or harm.

209. Carvin Software should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, the monetary value of the benefits that it unjustly received from Plaintiffs and Class Members.

FOURTH CAUSE OF ACTION
Violations of California's Unfair Competition Law ("UCL")
Unlawful Business Practice
Cal Bus. & Prof. Code § 17200, *et seq.*
(On behalf of Plaintiffs Lipp, Murray, Halpren and the California Subclass)

210. Plaintiffs Lipp, Murray and Halpren re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

211. Plaintiffs Lipp, Murray and Halpren, individually (hereinafter "Plaintiffs" for purposes of this Count only) and on behalf of the California Subclass, bring this claim.

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

213. Defendant engaged in unlawful business acts and practices by failing to establish adequate security practices and procedures as set forth above, by soliciting, gathering, and using for pecuniary gain the PII of Plaintiffs and the California Subclass knowing that the information would not be adequately protected, and by storing the PII of Plaintiffs and the California Subclass in an unsecure electronic system, all in violation of

California statutes, including Cal. Civ. Code § 1798.81.5, which require Defendant to undertake reasonable measures to safeguard the PII of Plaintiffs and the California Subclass, as well as the FTC Act and the CCPA.

214. Defendant's acts, omissions and misrepresentations, as alleged herein, were unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

215. Defendant's acts, omissions and misrepresentations, as alleged herein, were unlawful and in violation of the California Consumer Privacy Act which requires businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

216. Plaintiffs and California Subclass Members were within the class of persons the FTC Act and CCPA were intended to protect and the harm resulting from the data breach was the type of harm against which the statutes are intended to guard.

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

218. Moreover, Defendant's collection of sensitive PII in combination with its failure to implement reasonable security safeguards demonstrate Defendant's violation of the unfair prong of the UCL.

219. Defendant's acts and omissions were unfair in violation of the UCL. Defendant stored the PII of Plaintiffs and the California Subclass Members in its computer

systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiffs' and the California Subclass Members' PII secure and prevented the loss or misuse of that PII.

220. Plaintiffs and California Subclass Members were entitled to assume, and did assume, Defendant would take appropriate measures to keep their PII safe.

221. Defendant did not disclose to Plaintiffs or California Subclass Members at any time that their PII was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only entity in possession of that material information, which it had a duty to disclose.

222. Defendant violated the UCL by failing to maintain the safety of its computer systems, specifically the security thereof, and its ability to safely store Plaintiffs' and California Subclass Members' PII.

223. Defendant violated the unfair prong of the UCL by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and California Subclass Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and California Subclass Members' PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable and/or substantially injurious to Plaintiffs and California Subclass Members. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiffs and California Subclass Members outweighed their utility, if any.

224. 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 outweigh 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 Plaintiffs and California Subclass Members, directly causing the harms alleged below.

225. 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, therefore, amount to a violation of the law.

226. 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 thousands of California Subclass Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft,

disclosure of Plaintiffs' and California Subclass Members' PII to third parties without their consent, diminution in value of their PII, 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 Plaintiffs' and California Subclass Members' PII 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).

227. Plaintiffs and California Subclass Members have lost money and property as a result of Defendant's violations of the UCL as they were denied the benefit of their transacting with Defendant because Defendant failed to use funds from money paid by Plaintiffs and California Subclass Members to supply adequate data security. Moreover, Plaintiffs and California Subclass Members provided their PII to Defendant, which is property as defined by the UCL, and their property has been diminished in value as a result of the loss of its confidentiality.

228. Plaintiffs and California Subclass Members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. Plaintiffs' and

California Subclass Members' PII 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. Plaintiffs and California Subclass 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.

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

230. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur.

231. As such, Plaintiffs, on behalf of himself and California Subclass Members, seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

232. To the extent any of these remedies are equitable, Plaintiffs and the California Subclass seek such equitable remedies, in the alternative to any adequate remedy at law they may have.

FIFTH CAUSE OF ACTION
Violations of the California Consumer Privacy Act of 2018 ("CCPA")
Cal. Civ. Code § 1798, *et seq.*
(On behalf of Plaintiffs Lipp, Murray, Halpren and the California Subclass)

233. Plaintiffs, Lipp, Murray and Halpren, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

234. Plaintiffs, Lipp, Murray and Halpren, individually (hereinafter "Plaintiffs" for purposes of this Count only) and on behalf of the California Subclass, bring this claim.

235. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure.

236. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[23]

237. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable

[23] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

security procedures and practices that are appropriate to the nature of the information collected.

238. Defendant failed to implement such procedures which resulted in the Data Breach.

239. CCPA also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

240. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

241. Plaintiffs and the Class Members are "consumer[s]" as defined by Civ. Code § 1798.140(i) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by unique identifier."

242. Upon information and belief, Defendant is a "business" as defined by Civ. Code § 1798.140(d) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and either

d. has annual gross revenues in excess of $25 million; annually buys, sells, or shares, for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers or households; or derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

243. The PII taken in the Data Breach is personal information as defined by Civ. Code § 1798.81.5(d)(1)(A) because it contains Plaintiffs' and the Class members' unencrypted first and last names financial account information, and Social Security numbers.

244. Plaintiffs' and Class Members' PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including names and Social Security numbers, was wrongfully taken, accessed and viewed by unauthorized third parties.

245. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiffs' and the Class members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on their server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiffs' and Class Members' PII as a result of this attack.

246. On June 29, 2023, Plaintiff Murray, on behalf of himself and all other similarly situated Californians, provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). Defendant failed to respond within 30 days thereof and, upon information and belief has not cured or is unable to cure the violation. Accordingly, Plaintiffs seek all relief available under the CCPA, including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

247. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs seek injunctive relief, including public injunctive relief and declaratory relief.

SIXTH CAUSE OF ACTION
Violations Of the Tennessee Consumer Protection Act
Tenn. Code. Ann § 47-18-101, *et seq.*
(On behalf of Plaintiff Johnson and the Tennessee Subclass)

248. Plaintiff Johnson re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

249. Plaintiff Johnson, individually (hereinafter "Plaintiff" for purposes of this Count only) and on behalf of the Tennessee Subclass, brings this claim.

250. Tenn. Code Ann. § 47-18-109(a)(1) provides that "[a]ny person who suffers an ascertainable loss of money or property, real, personal, or mixed, or any other article, commodity, or thing of value wherever situated, as a result of the use or employment by another person of an unfair or deceptive act or practice described in § 47-18-104(b) and declared to be unlawful by this part, may bring an action individually to recover actual damage."

251. Tenn. Code Ann. § 47-18-109(a)(3) further provides that "[i]f the court finds that the use or employment of the unfair or deceptive act or practice was willful or knowing violation of this part, the court may award three (3) times the actual damages sustained and may provide such other relief as it considers necessary and proper…."

252. Defendant's consulting, staffing, payroll and billing services constitute "trade or commerce."

253. Defendant's conduct violates the Tennessee Consumer Protection Act because Defendant engaged in the deceptive acts and practices described above, which included a failure to protect Plaintiff's and the Tennessee Subclass's Personal Information.

254. Defendant omitted material facts concerning the steps they took (or failed to undertake) to protect Plaintiff and Tennessee Subclass members' PII, which were deceptive, false and misleading given the conduct described herein. Such conduct is inherently and materially deceptive and misleading in a material respect, which Defendant knew, or by the exercise of reasonable care, should have known, to be untrue, deceptive or

misleading. Such conduct is unfair, deceptive, untrue, or misleading in that Defendant: (a) represented that its services have approval, characteristics, uses or benefits that they do not have; and (b) represented that its services are of a particular standard, quality or grade.

255. Defendant's materially misleading statements and deceptive acts and practices alleged herein were directed at the public at large.

256. Defendant's actions impact the public interest because Plaintiff and the Tennessee Subclass have been injured in exactly the same way as thousands of others as a result of and pursuant to Defendant's generalized course of deception as described herein.

257. Defendant's acts and practices described above were likely to mislead a reasonable consumer acting reasonably under the circumstances.

258. Defendant's misrepresentations, misleading statements and omissions were materially misleading to Plaintiff and members of the Tennessee Subclass.

259. Defendant's violation of Tenn. Code Ann. § 47-18-104 was willful and knowing. As described above, at all relevant times, Defendant, among other things, knew that its policies and procedures for the protection of Plaintiff's and the Tennessee Subclass's PII were inadequate to protect that PII. Nonetheless, Defendant continued to solicit and process PII in the United States in order to increase its own profits.

260. Had Plaintiff and the members of the Tennessee Subclass known of Defendant's misrepresentations and omissions about their use of PII, they would not have permitted the use of Defendant's services and given Defendant or Defendant's clients their PII.

261. As a direct and proximate result of Defendant's conduct in violation of Tenn. Code Ann. § 47-18-104, Plaintiff and the members of the Tennessee Subclass have been injured in amounts to be proven at trial.

262. As a result, pursuant to Tenn. Code Ann. §§ 47-18-104 and 47-18-109, Plaintiff and the Tennessee Subclass are entitled to damages in an amount to be determined at trial. Plaintiff also properly asks that such damages be trebled based on Defendant's knowledge and/or intention with respect to the Breach.

263. Plaintiff also seeks injunctive relief, including a robust, state of the art notice program for the wide dissemination of a factually accurate statement on the actual state of Defendant's PII storage and the implementation of a corrective advertising campaign by Defendant.

264. Additionally, pursuant to Tenn. Code Ann. § 47-18-109, Plaintiff Johnson and the Tennessee Subclass make claims for attorneys' fees and costs.

SEVENTH CAUSE OF ACTION
Declaratory Judgment
(On behalf of Plaintiffs and the Class)

265. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

266. 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 FTCA as described in this Complaint.

267. Defendant owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' PII.

268. Defendant still possesses PII pertaining to Plaintiffs and Class Members.

269. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs 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.

270. 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 secure its customers' employees' PII under the common law and Section 5 of the FTCA;

b. Defendant's existing data security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect its customers' employees' PII; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure its customers' PII.

271. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect its customers' employees' PII, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security 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 on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing and training its security personnel regarding any new or modified procedures;

iv. 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;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii meaningfully educating its clients' employees about the threats they face with regard to the security of their PII, as well as the steps they should take to protect themselves.

272. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendant. The risk of another such breach is real, immediate and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

273. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs 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.

274. 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 at Defendant, thus, preventing future injury to Plaintiffs and others whose PII would be further compromised.

PRAYER FOR RELIEF

275. WHEREFORE Plaintiffs, on behalf of themselves and all others similarly situated, request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiffs as Class representative and the undersigned as Class counsel;

B. A mandatory injunction directing Defendant to adequately safeguard the PII of Plaintiffs and the Class hereinafter by implementing improved security procedures and measures, 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 business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete and purge the PII of Plaintiffs 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 Plaintiffs and Class Members;

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

v. requiring Defendant to engage independent, third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendant's systems on a periodic basis;

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

vii. requiring Defendant to conduct regular database scanning and securing checks;

viii. requiring Defendant to monitor ingress and egress of all network traffic;

ix. 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 PII, as well as protecting the PII of Plaintiffs and Class Members;

x. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs and systems for protecting personal identifying information;

xi. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated;

xii. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xiii. requiring Defendant to provide adequate credit monitoring to all Class Members.

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

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

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial;

I. For all other Orders, findings and determinations identified and sought in this Complaint; and

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

JURY TRIAL DEMANDED

Under Federal Rules of Civil Procedure 38(b), Plaintiffs demand a trial by jury for any and all issues in this action so triable as of right.

Date: August 4, 2023

Respectfully submitted,

/s/: William B. Federman

William B. Federman*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
-and-
212 W. Spring Valley Road
Richardson, Texas 75081

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Wills Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
abm@murphylegalfirm.com

Daisy Mazoff, Bar No. 028804
Mason A. Barney*
Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: dmazoff@sirillp.com
E: mbarney@sirillp.com
E: tbean@sirillp.com

Interim Co-Lead Counsel for Plaintiffs and the Proposed Class

Cristina Perez Hesano
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301
cperez@perezlawgroup.com

Interim Liaison Class Counsel for Plaintiffs and the Proposed Class

Gary M. Klinger**
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (202) 429-2290
gklinger@milberg.com

Kennedy M. Brian*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
kpb@federmanlaw.com

Raina C. Borrelli**
Samuel J. Strauss**
Brittany Resch**
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com
brittanyr@turkestrauss.com

Laura Grace Van Note*
Cody Alexander Bolce*
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone:(510) 891-9800

Facsimile: (510) 891-7030
Email: sec@colevannote.com
Email: lvn@colevannote.com

Jason M. Wucetich**
jason@wukolaw.com
Dimitrios V. Korovilas**
dimitri@wukolaw.com
WUCETICH & KOROVILAS LLP
222 N. Pacific Coast Hwy., Suite 2000
El Segundo, CA 90245
Telephone: (310) 335-2001
Facsimile: (310) 364-5201

Additional Attorneys for Plaintiffs and the Proposed Class

*Admitted *Pro Hac Vice*
** *Pro Hac Vice* Application Forthcoming