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

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Al Locke, Elijah Johnson, and Saeeda 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.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Al Locke, Elijah Johnson and Saeeda 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 "Private Information") from hackers.

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 Private Information of Plaintiffs and Class Members.

3. On or about May 2, 2023, Carvin Software filed official notice of data security incident with the Maine Attorney General. On or about the same time, Carvin Software also sent out data breach notice letters (the "Notice") to individuals whose Private Information was compromised as a result of the cyber attack.

4. Based on the Notice, Carvin Software detected unusual activity on some of its computer systems on or around March 29, 2023. Defendant's investigation revealed that an unauthorized party had access to certain company files, including the Private Information of Plaintiffs and over 187,000 other individuals, between February 22, 2023 and March 9, 2023 (the "Data Breach").

5. As a result of Defendant's inability to timely detect the Data Breach, Plaintiffs and "Class Members" (defined below) had no idea for *weeks* that their Private Information 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 imminet risk will remain for their respective lifetimes.

6. The Private Information 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.

7. Armed with the Private Information 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 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 Private Information, 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' Private Information 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' Private Information was a known risk to Carvin Software, and thus it was on notice that failing to take necessary steps to secure the Private Information 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 such systems that housed the Private Information. 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 as the Private Information 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 similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

15. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, breach of third-party beneficiary contract, unjust enrichment, and declaratory and injunctive relief.

II. PARTIES

16. Plaintiff Al Locke, is, and at all times mentioned herein was, an individual citizen of the State of Missouri.

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

18. Plaintiff Saeeda Johnson, is, and at all times mentioned herein was, an individual citizen of the State of Tennessee.

19. 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

20. 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

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

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

22. 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' Private Information

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

24. 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 and generates approximately $5 million in annual revenue.

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

26. 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' current and former employees' Private Information private; comply with industry standards related to data security and the maintenance of its customers' employees' Private Information; 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' Private Information; only use and release its customers' employees' Private Information for reasons that relate to the services it

provides; and provide adequate notice to its customers' employees if their Private Information is disclosed without authorization.

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

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

B. The Data Breach and Carvin Software's Inadequate Notice to Plaintiffs and Class Members

29. According to Defendant's Notice, it learned of unauthorized access to its computer systems on March 29, 2023, with such unauthorized access having taken place from at least February 22, 2023 to March 9, 2023.

30. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including Plaintiffs' and Class Members' names, Social Security numbers, and financial account information.

31. On or about May 2, 2023, Carvin Software finally began to notify customers that its investigation deterimined that their Private Information was compromised.

32. Carvin Software delivered the Notice to Plaintiffs and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "incident."

33. The notice letter 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.

34. Other than providing one year of crediting monitoring that Plaintiffs and Class Members would have to affirmatively sign up for, along with a call center number that victims could contact with questions, 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.

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

36. Plaintiffs and Class Members provided their Private Information 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.

37. 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 Private Information.

C. Carvin Software Failed to Comply with FTC Guidelines

38. 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 decisionmaking. 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).

39. 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.

40. 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.

41. 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.

42. 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' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

43. Carvin Software was at all times fully aware of its obligation to protect the Private Information of its customers 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

44. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

45. 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.

46. 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.

47. 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.

48. 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' Private Information

49. 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 Private Information 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 Private Information of Plaintiffs and Class Members.

50. 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' Private Information;

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' Private Information;

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' Private Information.

51. Carvin Software negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

52. 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 Private Information.

53. 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

54. 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.[1] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

[1] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on May 9, 2023).

55. 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.

56. 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.

57. 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.

58. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information 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.

59. 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.[2] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

60. 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.

61. 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.

62. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[3] The increase in

---

[2] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited May 9, 2023).

[3] *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-fourmembers-china-s-military (last visited on May 9, 2023).

cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

63. 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.[4] 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 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.[5]

64. 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 do 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."[6]

---

[4] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on May 9, 2023).

[5] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on May 9, 2023).

[6] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on May 9, 2023).

65. The Dark Web Price Index of 2022, published by PrivacyAffairs[7] shows how valuable just email addresses alone can be, even when not associated with a financial account:

2,400,000 million Canada email addresses	$100

66. 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.

67. Likewise, the value of PII is increasingly evident in our digital economy. Many companies collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[8]

68. 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."[9]

69. 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.

70. 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

---

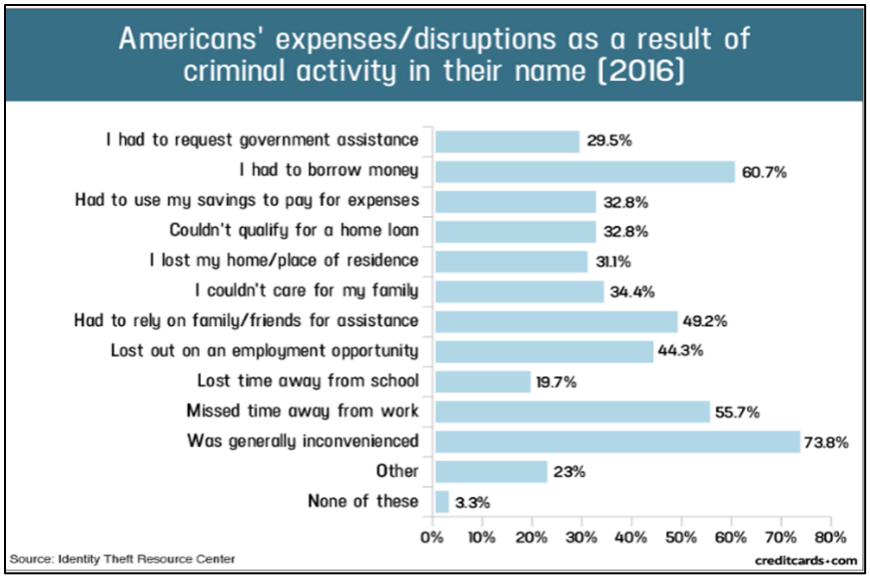
[7] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on May 9, 2023).

[8] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on May 9, 2023).

[9] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

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.

71. 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.



72. A study by the Identity Theft Resource Center[10] shows the multitude of harms caused by fraudulent use of PII:

73. 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

[10] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited May 9, 2023).

information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[11]

> [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.

74. 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.

75. 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. Plaintiffs' and Class Members' Damages

76. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

77. Plaintiffs and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services. In Plaintiff Locke's case, he entrusted his Private Information to Defendant through his employment with one of Defendant's clients, Paydayz Staffing. Plaintiffs Saeeda and Elijah Johnson entrusted their Private Information to Defendant through employment with Labor Exchange and Labor Smart.

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

---

[11] *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/270/262904.html (last visited May 9, 2023).

79. As a direct and proximate result of Carvin Software's actions and omissions, Plaintiffs and Class Members have been harmed and 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.

80. 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.

81. 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 Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

82. The Private Information 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 be and have been used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

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

84. 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.

85. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, 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.

86. 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 above.

V. CLASS ACTION ALLEGATIONS

87. Plaintiffs bring this action individually and on behalf of all other persons similar situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

88. Specifically, Plaintiffs propose the following Nationwide Class (referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
> All individuals in the United States who had Private Information stolen as a result of the Data Breach, including all who were sent a notice of the Data Breach.

89. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

90. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class and add subclasses before the Court determines whether certification is appropriate.

91. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

92. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 187,360 individuals whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Carvin Software's records, Class Members' records, publication notice, self-identification, and other means.

93. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Carvin Software engaged in the conduct alleged herein;

b. When Carvin Software learned of the Data Breach

c. Whether Carvin Software's response to the Data Breach was adequate;

d. Whether Carvin Software unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

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

f. Whether Carvin Software's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Carvin Software's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Carvin Software owed a duty to Class Members to safeguard their Private Information;

i. Whether Carvin Software breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether Carvin Software had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

l. Whether Carvin Software breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

m. Whether Carvin Software knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiffs and Class Members suffered as a result of Carvin Software's misconduct;

o. Whether Carvin Software's conduct was negligent;

p. Whether Carvin Software's conduct was *per se* negligent;

q. Whether Carvin Software was unjustly enriched;

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

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

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

94. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

95. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

96. Predominance. Carvin Software has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Carvin Software's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

97. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions

of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Carvin Software. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

98. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Carvin Software has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

99. Finally, all members of the proposed Class are readily ascertainable. Carvin Software has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Carvin Software.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class)

100. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

101. Carvin Software knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

102. Carvin Software's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

103. Carvin Software knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Carvin Software was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

104. Carvin Software owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Carvin Software's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect its customers' employees' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

105. Carvin Software's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which

prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

106. Carvin Software's duty also arose because Defendant was bound by industry standards to protect its customers' employees' confidential Private Information.

107. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Carvin Software owed them a duty of care to not subject them to an unreasonable risk of harm.

108. Carvin Software, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within its possession.

109. Carvin Software, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

110. Carvin Software, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

111. Carvin Software breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA; and

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised.

112. Carvin Software acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

113. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices on the part of Defendant. Plaintiffs and Class Members had no ability to protect their Private Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

114. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that Plaintiffs and the Class had entrusted to it.

115. Carvin Software's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

116. Carvin Software's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

117. As a result of Carvin Software's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

118. As a direct and proximate result of Carvin Software's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent

risk of further harm. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

119. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

120. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring Carvin Software to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

121. Plaintiffs restate and reallege the allegations in paragraphs 1-99 as if fully set forth herein.

122. Defendant entered into contracts, written or implied, with its clients to perform services that include, but are not limited to, providing staffing software and other services. Upon information and belief, these contracts are virtually identical between and among Defendant and its customers around the country whose employees, including Plaintiffs and Class Members, were affected by the Data Breach.

123. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiffs and the Class.

124. These contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that if it were to breach these contracts with its clients, the clients' employees—Plaintiffs and Class Members—would be harmed.

125. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' Private Information from

unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiffs and Class Members thereof.

126. Plaintiffs and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

127. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

128. Plaintiffs restate and reallege the allegations in paragraphs 1-99 as if fully set forth herein.

129. This Count is pleaded in the alternative to Count II above.

130. Plaintiffs and Class Members conferred a benefit on Carvin Software by turning over their Private Information to Defendant and utilizing its services directly or indirectly through their respective employers to whom Plaintiffs and Class Members entrusted their Private Information and who subsequently transmitted such Private Information to Defendant.

131. As a result of Plaintiffs' and Class Members use of Defendant's services as set forth herein, Defendant received monetary benefits and the use of the valuable Private Information entrusted to it for business purposes and financial gain.

132. Defendant collected, maintained, and stored the Private Information of Plaintiff and Class Members and, as such, had direct knowledge of the monetary benefits conferred upon it (including the use of the valuable Private Information for business purposes and financial gain) by the entities that collected Plaintiffs' and Class Members' Private Information and that used Defendant's services.

133. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with the entities that collected

Plaintiffs' and Class Members' Private Information, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on reasonable data privacy and security measures to secure Plaintiffs' and Class Members' Personal Information.

134. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Private Information, Defendant, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiffs and Class Members.

135. If Plaintiffs and Class Members had known that Carvin Software would not adequately secure their Private Information, they would not have agreed to provide such Private Information to Defendant.

136. Due to Carvin Software's conduct alleged herein, it would be unjust and inequitable under the circumstances for Carvin Software to be permitted to retain the benefit of its wrongful conduct.

137. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Carvin Software's possession and is subject to further unauthorized disclosures so long as Carvin Software fails to undertake appropriate and adequate measures to protect Private Information in its

continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

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

COUNT IV
DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Nationwide Class)

140. Plaintiffs restate and reallege the allegations in paragraphs 1-99 as if fully set forth herein.

141. 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.

142. Carvin Software owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

143. Carvin Software still possesses Private Information pertaining to Plaintiffs and Class Members.

144. Plaintiffs allege that Carvin Software's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise

of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

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

a. Carvin Software owes a legal duty to secure its customers' employees' Private Information under the common law and Section 5 of the FTCA;

b. Carvin Software'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' Private Information; and

c. Carvin Software continues to breach this legal duty by failing to employ reasonable measures to secure its customers' employees' Private Information.

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

a. Order Carvin Software 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, Carvin Software 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 Carvin Software's systems on a periodic basis, and ordering Carvin Software 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 Carvin Software'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 Private Information, as well as the steps they should take to protect themselves.

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

148. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Carvin Software 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 Carvin Software's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Carvin Software has a pre-existing legal obligation to employ such measures.

149. 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 Carvin Software, thus preventing future injury to Plaintiffs and others whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Carvin Software to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Carvin Software to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: May 10, 2023

Respectfully submitted,

Daisy Mazoff
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

ClassAction.org